

全国计算机技术与软件专业技术资格（水平）考试参考用书

# 网络管理员考试同步辅导

## （下午科目）

工业和信息化部教育与考试中心　推荐

何淑娟 江明星 主编 / 赵卫 杨立功 副主编

第3版

清华大学出版社

全国计算机技术与软件专业技术资格(水平)考试参考用书

# 网络管理员考试同步辅导

## (下午科目)(第 3 版)

何淑娟　江明星　赵　卫　杨立功　主编

清华大学出版社
北　京

## 内 容 简 介

本书是按照现人力资源和社会保障部、工业和信息化部最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲和指定教材编写的考试辅导书。全书共分为5章，内容包括小型局域网的构建与综合布线、局域网服务器的安装和配置、网络安全设置、网络管理与故障处理、Web网站建设，主要从考试大纲要求、考点辅导、典型例题分析、本章小结和达标训练几个方面对各部分内容加以系统阐释。

本书具有考点分析透彻、例题典型、习题丰富等特点，非常适合备考网络管理员的考生使用，也可作为高等院校或培训班的教材。



**图书在版编目(CIP)数据**

网络管理员考试同步辅导(下午科目)/何淑娟，江明星主编. —3版. —北京：清华大学出版社，2018
(全国计算机技术与软件专业技术资格(水平)考试参考用书)
ISBN 978-7-302-50549-5

Ⅰ. ①网…　Ⅱ. ①何…　②江…　Ⅲ. ①计算机网络管理—资格考试—自学参考资料　Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2018)第145343号

**责任编辑**：魏　莹　李玉萍
**装帧设计**：常雪影
**责任校对**：周剑云
**责任印制**：杨　艳
**出版发行**：清华大学出版社
**网　　址**：http://www.tup.com.cn, http://www.wqbook.com
**地　　址**：北京清华大学学研大厦A座　　**邮　　编**：100084
**社 总 机**：010-62770175　　**邮　　购**：010-62786544
**投稿与读者服务**：010-62776969, c-service@tup.tsinghua.edu.cn
**质量反馈**：010-62772015, zhiliang@tup.tsinghua.edu.cn
**印 装 者**：三河市君旺印务有限公司
**经　　销**：全国新华书店
**开　　本**：185mm×260mm　**印　张**：17.75　**插　页**：2　**字　数**：428千字
**版　　次**：2005年8月第1版　2018年9月第3版　**印　次**：2018年9月第1次印刷
**定　　价**：56.00元

---

产品编号：071201-01

# 再版前言

全国计算机技术与软件专业技术资格(水平)考试自实施起至今已经历了 20 多年，在社会上产生了很大的影响，其权威性得到社会各界的广泛认可。为了适应我国信息化发展的需求，人事部(现为人力资源和社会保障部)、信息产业部(现为工业和信息化部)在 2004 年决定将考试的级别拓展到计算机技术与软件各个方面，将网络程序员级别考试改为网络管理员级别考试，2009 年又对网络管理员级别考试大纲进行了重新调整，以满足社会对各种信息技术人才的需要。本书第 1 版自 2005 年出版以来，被众多考生选用为考试参考教材，多次重印，深受广大读者好评。2013 年对第 1 版进行了修订。为了帮助考生复习迎考，根据最新的考试大纲及网络新技术的发展，本书对第 2 版进行修订。主要修订内容如下。

(1) 知识点更新。本书在第 2 版的基础上，严格按照最新版大纲，对知识点做了调整，更符合考试大纲对考试的要求。

(2) 结构调整。参考最新指定官方教程、最新考试大纲及最新题型编写章名、节名，便于考生使用《网络管理员教程(第 5 版)》同步复习，同时更加突出重点与难点，针对性强，可减轻考生复习的工作量。

(3) 例题与习题更新。对书中原有例题与习题进行了彻底更新，将最近 4 年(2014—2017 年)8 次考试真题全部分类解析到例题中，并在其中增加了根据最新考试大纲精心设计的例题，这些例题均具有典型性和代表性，而将 2013 年两次考试真题全部分类归入同步练习中。这样考生能从以前的考题中更好地了解考试的难度与广度。

(4) 更加突出重点。第 3 版沿袭前一版的框架，每一小节分为 4 个模块：考点辅导、典型例题分析、同步练习、同步练习参考答案。其中，考点辅导部分主要以专题的方式，重点介绍网络管理员上午考试所需的各个方面的知识；典型例题分析是本书的重点，它详尽细致地剖析了所有近 4 年(2014—2017 年)的真题和例题；同步练习中的每一道题都配有标准答案；此外，每章还配有一定数量的习题及答案，对读者所学的知识和能力可起到巩固、拓展和提高的作用。

(5) 概念更清晰，能覆盖所有大纲考点，并突出重难点。

(6) 精选书中所有例题与习题，确保所有题目符合考纲要求。例题选取典型、有梯度、有广度，分析更详尽；题目的难易度、分布率与真实考试相当；题目答案正确、解析科学；无重复题目、雷同题目。

本书非常适合备考网络管理员的考生使用，也可作为高等学校相关专业或培训班的教材。

本书第 1 版由李文龙、施宁、陶安、俞永达、张伍荣等编写。第 2 版由杨立功、江明星等编写。第 3 版由何淑娟、江明星、赵卫、杨立功编写和修订，参与本书组织、编写和

资料收集的还有崔艳春、陈亚天、任立涛、左从菊、朱明、朱锦龙、闫鸿滨、杨继琼、高云、卫星、张德成、刘綦、何光明等。在此对原作品的全体参与人员表示衷心的感谢。

在本书的编写过程中，参考了许多相关的书籍和资料，目录详见参考文献，本书从中汲取了许多营养，在此表示感谢。需要特别提出感谢的是来自互联网的一些不知姓名的网友们的无私奉献，正是由于你们，才使本书的内容更完善、更详尽。

由于作者水平所限，书中难免存在错漏和不妥之处，敬请广大读者批评指正。

编　者

# 网络管理员考试(下午)考点分布导航图

| 章 | 节 | 历年真题分布 | | | | | | | | 大纲要求 | 阅读链接 | 命题预测 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2014.05 | 2014.11 | 2015.05 | 2015.11 | 2016.05 | 2016.11 | 2017.05 | 2017.11 | | | |
| 第 1 章 小型局域网的构建与综合布线 | 1.1 局域网组网的设计 | 相关考题结合“1.2 局域网组网技术及设备选择”一起考 | | | | | | | | ①组网技术选择<br>②组网设备选择及部署<br>③设备配置和管理<br>④划分 VLAN<br>⑤综合布线<br>⑥IP 地址、子网掩码的规划配置<br>⑦网络规划<br>⑧命令行接口访问交换机和路由器<br>⑨Web 方式访问交换机和路由器<br>⑩VLAN 配置<br>⑪路由器路由协议配置<br>⑫广域联网 | **1. 考题分布**<br>通常出现在网络管理员考试(下午科目)的第 1 题或者第 2 题<br>**2. 阅读提示**<br>本章的“1.1 局域网组网的设计”，“1.2 局域网组网技术及设备选择”，“1.3 以太网交换机的部署”和“1.4 交换机与路由器的基本配置”对应《网络管理员教程(第 5 版)》(以下简称“教程”)的“3.2 以太网”、“3.3 交换机与路由器的基本配置”和“3.4 综合布线”，“1.5 IP 地址及其规划”对应教程的“1.4.3 IP 地址”。考生可以对照教程相关内容进行同步复习<br>**3. 补充说明**<br>但需要注意的是，增加了大纲未明确指出、教程未提及，但考试中遇到的重要考点：<br>※组网设备选择及部署，请考生留意此部分内容 | 本章节考点分值约占总考分的 12%。考查在指定网络环境要求下进行网络设计，包括设计拓扑结构、所用的设备类型、线缆类型、网络排错等。有时也考查对原网络的升级。高频考点为：<br>◆局域网组网技术及设备选型<br>◆交换机和路由器的基本配置<br>◆IP 地址以及子网掩码的规划 |
| | 1.2 局域网组网技术及设备选择 | 路由器和交换机(2 分) | 路由器和交换机(3 分) | | 路由器和交换机(4 分)，双绞线(3 分) | | 交换机(2 分) | 路由器和交换机(4 分) | 路由器和交换机(4 分) | | | |
| | 1.3 以太网交换机的部署 | 交换机的控制台端口(2 分) | 交换机的控制台端口(2 分) | 交换机的控制台端口(2 分) | | 交换机的控制台端口(2 分) | | 交换机的控制台端口(2 分) | 交换机的控制台端口(2 分) | | | |
| | 1.4 交换机与路由器的基本配置 | 2009 年考试大纲新增加的内容，至今还没有出过考题。 | | | | | | | | | | |
| | 1.5 综合布线 | 2009 年考试大纲弱化的知识点，至今还没有出过考题。 | | | | | | | | | | |
| | 1.6 IP 地址及其规划 | IP 地址及子网掩码(6 分) | 路由表(4 分) | 配置 Internet 协议属性参数(15 分) | IP 地址及子网掩码(4 分) | | IP 地址及子网掩码(13 分) | IP 地址及子网掩码(11 分) | IP 地址及子网掩码(8 分)，路由表(5 分) | | | |

续表

| 章 | 节 | 历年真题分布 | | | | | | | | 大纲要求 | 阅读链接 | 命题预测 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2014.05 | 2014.11 | 2015.05 | 2015.11 | 2016.05 | 2016.11 | 2017.05 | 2017.11 | | | |
| 第 2 章 局域网服务器的安装和配置 | 2.1 操作系统的安装 | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | Windows Server 2003 的安装(15 分) | ①Windows DNS 服务器的配置和维护<br>②Windows 电子邮件服务器的配置和维护<br>③Windows FTP 服务器的配置和维护<br>④Windows 代理服务器的配置和维护<br>⑤Windows DHCP 服务器的配置和维护<br>⑥Windows Web 服务器的配置和维护 | **1. 考题分布**<br>通常出现在网络管理员考试(下午科目)的第 2 题或者第 3 题，也偶尔出现在第 1 题<br>**2. 阅读提示**<br>本章的“2.1 操作系统的安装”对应教程“4.2 Windows Server 2008 R2 的安装与配置”和“4.3 Red Hat Enterprise Linux 7”；“2.2 DNS 服务器配置”对应教程“5.2 DNS 服务器的配置”；“2.3 电子邮件服务”对应教程“2.3 电子邮件”；“2.4 FTP 服务器”和“2.5 Web 服务器配置”对应教程“5.1 IIS 服务器配置”；“2.7 DHCP 服务器的配置”对应教程“5.3 DHCP 服务器的配置”。考生可以对照教程的相关内容进行同步复习 | 本章节考点分值约占总考分的 43%。考生应充分重视本章的复习。通常考查各种服务器的配置实现。高频考点为：<br>◆常见操作系统的安装<br>◆Windows FTP 服务器的配置<br>◆Windows DNS 服务器的配置<br>◆ Windows DHCP 服务器的配置 |
| | 2.2 DNS 服务器配置 | Windows Server 2003 系统 DNS 服务器的配置过程(13 分) | | | Windows Server 2003 系统 DNS 服务器的配置过程(13 分)，测试 DNS 配置成功情况(2 分) | | | 域名服务器的类型(3 分)，域名服务器的功能(3 分)，DNS 服务的启动和停止(4 分)，域名服务器的配置(3 分)，DNS 故障排除(2 分) | | | | |
| | 2.3 电子邮件服务 | | | | | | | 电子邮件服务器的配置过程(15 分) | | | | |
| | 2.4 FTP 服务器 | FTP 服务器的端口(3 分)，配置 FTP 服务器的过程(6 分)，连接 FTP 服务器的命令(6 分) | | | FTP 协议和 TCP 协议(4 分)，FTP 服务器的端口(4 分)，vsftp 服务(7 分) | | | | FTP 服务器的配置过程(11 分)，测试 FTP 服务器配置成功情况(4 分) | | | |
| | 2.5 Web 服务器配置 | Web 服务器的配置过程(4 分) | Web 服务器的配置过程(2 分) | | | Web 服务器的配置过程(5 分) | | Web 服务器的配置(7 分) | Web 服务器的功能(2 分) | | | |
| | 2.6 代理服务器配置 | | Linux 网卡的配置过程(15 分) | | | 代理服务器软件(2 分)，代理服务器的配置过程(13 分) | | | | | | |
| | 2.7 DHCP 服务器配置 | DHCP 服务的工作过程(6 分)，DHCPServer 配置属性参数(7 分) | | DHCP 服务的工作过程(4 分)，DHCPServer 配置属性参数(7 分) | | DHCP 服务的工作过程(4 分)，DHCPServer 配置属性参数(7 分) | | DHCP 工作流程(6 分)，DHCP Server 配置属性参数(4 分)，设置 Internet 协议属性参数(1 分)，PCI 重新租用 IP 地址的命令(4 分) | | | | |

续表

| 章 | 节 | 历年真题分布 | | | | | | | | 大纲要求 | 阅读链接 | 命题预测 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2014.05 | 2014.11 | 2015.05 | 2015.11 | 2016.05 | 2016.11 | 2017.05 | 2017.11 | | | |
| 第3章网络安全设置 | 3.1 网络病毒防护策略和入侵处理策略 | | 木马程序的特点(4分)，入侵处理策略(6分)，网络病毒防护策略(3分) | | | | | | | ①防火墙的配置策略<br>②入侵处理策略<br>③漏洞处理策略<br>④病毒及病毒防范<br>⑤DES和RSA的基本概念<br>⑥认证<br>⑦数字证书<br>⑧安全电子邮件<br>⑨HTTPS | **1. 考题分布**<br>通常出现在网络管理员考试(下午科目)的第4题<br>**2. 阅读提示**<br>本章对应教程"7.1 网络安全基础"、"7.8 防火墙"和"7.9 网络防病毒系统"。考生可以对照教程相关内容进行同步复习<br>**3. 补充说明：**<br>教程内容已经基本覆盖大纲要求的考点，但需要注意的是增加了大纲未明确指出、教程未提及，但考试中遇到的重要考点：<br>访问控制列表；<br>SSL与TCP/IP协议之间的关系 | 本章节考点分值约占总考分的15%。考查针对一个网络环境来部署防火墙，如在网络中防火墙的连接位置、网络中不同部分的IP地址的配置等。并考查配置防火墙的规则(如源和目标的IP地址、通信协议、通信端口、数据传输的方向、通信允许或拒绝等)。高频考点为：<br>◆网络病毒的防护策略<br>◆网络病毒的特点<br>◆入侵处理策略<br>◆防火墙的基本配置<br>◆访问控制列表<br>◆漏洞处理策略 |
| | 3.2 防火墙的配置策略和漏洞处理策略 | | 防火墙的功能(2分) | 防火墙的类型和基本结构(3分)，防火墙内部的连接方式和设备(3分)，防火墙的功能(3分)，防火墙访问控制规则的配置(4分)，防火墙的地址隐藏功能配置(2分) | HTTPS的概念(2分)，SSL(13分) | | | 防火墙的安全区域(2分)，包过滤防火墙的功能(2分)，ACL语句(8分)，防火墙的配置过程(3分) | 配置NAT/基本防火墙的过程(15分)，防火墙的安全区域(4分) | | | |
| 第4章网络管理与故障处理 | 4.1 网络管理软件 | 常见网络管理命令(7分) | 常见网络管理命令(6分) | 常用网络管理命令(4分) | | | | 常用网络管理命令(13分) | 常用网络管理命令(4分) | ①使用网络管理软件对网络的配置、安全、性能、故障、计费进行监督和管理<br>②简单网络故障的分析、定位、诊断和排除<br>③小型网络的维护策略、计划和实施<br>④数据备份和数据恢复<br>⑤系统性能分析 | **1. 考题分布**<br>通常出现在网络管理员考试(下午科目)的第3题，也偶尔出现在第1题<br>**2. 阅读提示**<br>本章对应教程的"8.1 网络管理简介""8.2 简单网络管理协议""8.3 网络管理工具"和"8.4 基于Windows的网络管理"。考生可以对照教程相关内容进行同步复习 | 本章节考点分值约占总考分的10%。根据相关的故障现象来判断故障原因并排除故障。高频考点为：<br>◆常见的网络管理命令格式<br>◆常用故障排除的方法<br>◆网络故障的诊断 |
| | 4.2 网络故障 | 网络故障诊断(2分) | 常见的网络故障诊断(4分)，SNMP服务知识(15分) | SNMP服务知识(5分) | 常见的网络故障诊断(2分)，SNMP服务知识(5分) | SNMP服务知识(5分) | SNMP服务知识(10分) | 网络故障排除(4分)，常见网络故障的排除(2分) | Web故障排除(2分)，网络病毒故障诊断(3分)，代理服务器故障诊断(2分) | | | |

续表

| 章 | 节 | 历年真题分布 | | | | | | | | 大纲要求 | 阅读链接 | 命题预测 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 2014.05 | 2014.11 | 2015.05 | 2015.11 | 2016.05 | 2016.11 | 2017.05 | 2017.11 | | | |
| 第 5 章 Web 网站建设 | 5.1 用 HTML 制作网页 | 相关考题一般结合“5.2 动态网页制作”一起考 | | | | | | | | ①Web 网站的规划、建设、管理与维护<br>②HTML 网页设计与制作<br>③JSP、ASP 动态网页编程技术<br>④ADO 的概念和使用 | **1. 考题分布**<br>固定出现在网络管理员考试(下午科目)的第 5 题<br>**2. 阅读提示**<br>本章对应教程的“6.1 使用 HTML 制作网页”“6.3 网页制作工具”“6.4 动态网页的制作”以及“6.6 Web 网站创建与维护”。考生可以对照教程相关内容进行同步复习 | 本章节考点分值约占总考分的 20%，考生应充分重视本章的复习。通常以程序填空的形式来完成具有指定功能的网页。高频考点为:<br>◆HTML 常用元素<br>◆ASP 内嵌对象 |
| | 5.2 动态网页制作 | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | ASP 动态网页制作基础知识(15 分) | | | |
| | 5.3 Web 网站的创建与维护 | 相关考题一般结合“5.1 用 HTML 制作网页”和“5.2 动态网页制作”一起考 | | | | | | | | | | |

# 目　录

# 第 1 章　小型局域网的构建与综合布线

**大纲要求：**

- 小型计算机局域网的构建，包括网络规划、组网技术选择、组网设备选择及部署、设备配置和管理、划分 VLAN、综合布线系统。
- 交换机和路由器的基本配置，包括命令行接口访问交换机和路由器、Web 方式访问交换机和路由器、VLAN 配置、路由器路由协议配置、广域联网。

## 1.1　局域网组网的设计

### 1.1.1　考点辅导

#### 1.1.1.1　局域网的设计原则

设计局域网时应遵循以下原则。

1. 实用性原则

网络系统应采用成熟、可靠的技术和设备，这样才能做到实用、经济和有效。

2. 开放性原则

网络系统应采用开放的标准和技术。

3. 可靠性原则

网络系统应确保很高的可靠性，具有较高的平均无故障时间和较低的平均故障率。

4. 安全性原则

网络系统应具有良好的安全性，以确保网络系统和数据的安全运行。

5. 先进性原则

网络系统应采用先进的技术和设备，以符合网络未来发展的潮流。

6. 高效性原则

网络系统应具有很高的资源利用率。

7. 可扩展性原则

网络系统应在规模和性能两个方面具有良好的可扩展性。

8. 高性价比原则

网络系统应具有较高的性价比，技术优先，兼顾价格。

#### 1.1.1.2 局域网的设计步骤

1. 网络需求分析

在组建局域网之前首先要进行需求分析工作，根据用户提出的要求进行网络设计。网络建设的成败很大一部分取决于网络实施前的规划工作。

1) 网络的功能要求

任何网络都不可能是一个能够满足各项功能需求的“万能网”。因此，必须针对每个具体的网络所要完成的功能，依据使用需求、实现成本、未来发展、总预算投资等因素对网络的组建方案进行认真的设计和推敲。

2) 网络的性能要求

对网络系统处理的性能进行分析，根据网络的工作站权限、容错程度、网络安全性方面等要求，确定采取何种措施及方案。

3) 网络运行环境的要求

根据整个局域网运行时所需要的环境要求，确定使用哪种网络操作系统、应用软件和共享资源。

4) 网络的可扩展性和可维护性要求

如何增加工作站、怎样与其他网络联网、对软件/硬件的升级换代有何要求与限制等，都要在网络设计时加以考虑，以保证网络的可扩展性和可维护性。

2. 确定网络类型和带宽

与其他网络技术相比，以太网具有价格低、可靠性高、可扩展性好、易于管理等优点，所以一般局域网都选择以太网。根据局域网接入计算机的数量及规模可确定网络带宽和交换设备，目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量达到数百台或网络数据流量比较大的情况下，应采用千兆以太网技术，以满足对网络主干数据流量的要求。网络主干和分支方案确定以后，就可以选择集线器或交换机产品了。集线器或交换机的型号与数量由联入网络的计算机数量和网络拓扑结构来决定。

3. 确定网络设备

网络设备的选择应遵循以下原则。

1) 厂商的选择

所有网络设备尽可能选取同一厂家的产品，这样在设备的可互联性、协议互操作性、技术支持、价格等方面更有优势。

2) 可扩展性考虑

在网络的层次结构中，主干设备应预留一定的可扩展能力，而低端设备则够用即可，因为低端设备更新较快且易于扩展。

3) 根据方案实际需要选型

在参照整体网络设计要求的基础上，根据网络实际带宽性能需求、端口类型和端口密度选择。如果是旧网改造项目，则应尽可能保留并延长用户对原有网络设备的投资，减少在资金投入方面的浪费。

4)　选择性价比高、质量过硬的产品

为了使资金的投入与产出能达到最大值，能以较低的成本、较少的人员投入来维护系统运转，网络开通后能运行许多关键业务，要求系统具有较高的可靠性。

4. 确定布线方案和布线产品

现在的布线系统主要是光纤和非屏蔽双绞线，小型网络多以超五类非屏蔽双绞线为布线系统，因为布线是一次性工程，因此应考虑在未来几年内网络可扩展的最大点数。

5. 确定服务器和网络操作系统

服务器是网络数据储存的仓库，其重要性可想而知。服务器的类型和档次应与网络的规模、数据流量以及可靠性要求相匹配。

如果是几十台计算机以下的小型网络，并且数据流量不大，选用入门级服务器基本上可以满足需要；如果是数百台左右的中型网络，则应选用工作组级服务器；如果是上千台的大型网络，则应选用企业级服务器。

服务器的数量由网络应用来决定，可以根据实际情况配备 E-mail 服务器、Web 服务器、数据库服务器等，也可以让一台服务器充当多种服务器角色。

目前，网络操作系统基本上是三分天下：微软的 Windows 2000 Server、传统的 UNIX 和 Linux，可以根据网络规模、技术人员水平、资金等综合因素来决定究竟使用什么网络操作系统。

6. 其他

局域网的设计还包括不间断电源、网络安全、互联网接入、网络应用系统等方面的设计。

## 1.1.2　典型例题分析

**例**　请简要回答以下局域网设计时的有关问题。

**【问题 1】**简述设计网络系统时需遵循的基本原则。

**【问题 2】**局域网的硬件设备目前大多选择什么网络设备?

**【问题 3】**以太网的特点是什么?

**【问题 4】**局域网设计与连接时考虑的主要因素是什么?

**分析：**设计局域网时应遵循以下原则，即实用性原则、开放性原则、可靠性原则、安全性原则、先进性原则、高效性原则、可扩展性原则和高性价比原则。

以太网技术是目前局域网技术中最成熟的技术，所以局域网的硬件设备大多选择以太网的网络设备。以太网的特点如下。

(1)　开放标准，获得众多厂商的支持。目前，几乎所有的硬件制造商生产的设备和几乎所有的软件开发商的操作系统和应用协议都与以太网兼容。

(2)　易于移植和升级，可最大限度地保护用户投资。对于所有以太网技术，其帧的结

构几乎是一样的，这就提供了非常好的升级途径。快速以太网技术提供了从 10Mb/s 向 100Mb/s 以太网的平滑升级。千兆位和万兆位以太网的出现，在增加带宽的同时也扩展了可升级性。只要将低速以太网设备用交换机连接到千兆位或万兆位以太网的设备上，就可实现一个物理线速向另一物理线速的适配。这样的升级方式就使得千兆位和万兆位以太网能无缝地与现在的以太网集成在一起。

(3) 价格便宜，管理成本低。以太网技术在价格上与其他技术相比具有优越性。若全面采用以太网技术解决方案，价格将更具有吸引力。另外，以太网存在时间长，标准化程度高，一般网络管理人员都比较熟悉，因此它的运行维护管理成本也比较低。

(4) 结构简单，组网方便。以太网技术的实现原理统一采用了 CSMA/CD 媒体访问控制方法，不同版本的以太网帧结构和网络拓扑结构也是一致的，对布线系统的要求较低，网络连接设备的配置比较简单。

所以一般局域网都选择以太网。根据局域网接入计算机的数量及规模可确定网络带宽和交换设备，目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量达到数百台或在网络数据流量比较大的情况下，应采用千兆位以太网技术，以满足对网络主干数据流量的要求。网络主干和分支方案确定之后，就可以选定集线器或交换机产品了。集线器或交换机的数量由联入网络的计算机数量和网络拓扑结构来决定。

**答案：**

**【问题 1】**设计网络系统时应遵循实用性原则、开放性原则、可靠性原则、安全性原则、先进性原则、高效性原则、可扩展性原则和高性价比原则。

**【问题 2】**以太网。

**【问题 3】**以太网具有开放标准，获得众多厂商的支持；易于移植和升级，最大限度地保护用户投资；价格便宜，管理成本低；结构简单，组网方便等特点。

**【问题 4】**网络类型和带宽。

## 1.1.3 同步练习

如何确定局域网的服务器？局域网常使用的操作系统有哪些？

## 1.1.4 同步练习参考答案

服务器是网络数据储存的仓库，其重要性可想而知。服务器的类型和档次应与网络的规模和数据流量以及可靠性要求相匹配。如果是几十台计算机以下的小型网络，而且数据流量不大，选用入门级服务器基本上可以满足需要；如果是数百台左右的中型网络，选用工作组服务器；如果是上千台的大型网络，选用企业级服务器。

局域网常使用的操作系统有微软的 Windows Server、UNIX 和 Linux。

# 1.2　局域网组网技术及设备选择

## 1.2.1　考点辅导

### 1.2.1.1　局域网基础

1. *局域网参考模型*

局域网体系结构由物理层、媒体访问控制子层(MAC)和逻辑链路控制子层(LLC)组成。

IEEE 802 参考模型的最底层对应于 OSI 模型中的物理层，具体包括以下功能。

(1) 信号的编码/解码。

(2) 前导码的生成/去除(前导码仅用于接收同步)。

(3) 位的发送/接收。

IEEE 802 参考模型的 MAC 子层和 LLC 子层合起来与 OSI 模型中的数据链路层相对应。MAC 子层完成的功能如下。

(1) 在发送时将要发送的数据帧组装成帧，帧中包含地址和差错检测等字段。

(2) 在接收时将接收到的帧解包，并进行地址识别和差错检测。

(3) 管理和控制对于局域网的传输媒体的访问。

LLC 子层完成的功能如下。

(1) 为高层协议提供相应的接口，即一个或多个服务访问点(SAP)，通过 SAP 支持面向连接的服务和复用能力。

(2) 端到端的差错控制和确认，确保无差错传输。

(3) 端到端的流量控制。

需要指出的是，在局域网中采用了两级寻址，用 MAC 地址标识局域网中的一个站，LLC 提供了服务访问点地址，SAP 指定了运行于一台计算机或网络设备上的一个或多个应用进程地址。

2. *局域网拓扑结构*

按照不同的物理布局，局域网的拓扑结构通常可分为 3 种，分别是总线型拓扑结构、星型拓扑结构和环型拓扑结构。

总线型结构是使用同一媒体或电缆连接所有端用户的一种方式，也就是说，连接端用户的物理媒体由所有设备共享。

星型结构有中心节点，各节点通过点对点的方式与中心节点相连，任何两个节点之间的通信都要通过中心节点来转接。

环型结构在 LAN 中使用较多。这种结构的传输媒体从一个端用户连接到另一个端用户，直到将所有端用户连成环形。

3. *局域网媒体访问控制方法*

目前，计算机局域网常用的访问控制方式有 3 种，分别是载波侦听多路访问/冲突检

测(CSMA/CD)法、令牌环(Token Ring)访问控制法和令牌总线(Token Bus)访问控制法。

CSMA/CD 包含两方面内容，即载波侦听(CSMA)和冲突检测(CD)。CSMA/CD 访问控制方式主要用于总线型网络拓扑结构，是 IEEE 802.3 局域网标准的主要内容。

Token Ring 是令牌通行环的简写。其主要技术指标是：网络拓扑为环型布局，基带网，数据传送速率为 4Mb/s，采用单个令牌(或双令牌)的令牌传递方法。环型网络的主要特点是：只有一条环路，信息单向沿环流动，无路径选择问题。

Token Bus 是令牌通行总线(Token Passing Bus)的简写。这种方式主要用于总线型或树型网络结构中。1976 年美国 Data Point 公司研制成功的 ARCnet(Attached Resource Computer network)网络综合了令牌传递方式和总线网络的优点，在物理总线结构中实现令牌传递控制方法，从而构成一个逻辑环路。此方式也是目前计算机局域网中的主流介质访问控制方式。

#### 1.2.1.2　无线局域网简介

1. 无线数据网络的种类

无线数据网络解决方案包括无线个人网、无线局域网、无线城域网和无线广域网。

无线个人网主要用于个人用户工作空间，典型的覆盖距离为几米，可与计算机同步传输文件，访问本地外围设备，通常被形容为满足“最后 10 米”的通信需求，目前的主要技术为蓝牙(Bluetooth)技术。

无线局域网(Wireless LAN，WLAN)是一种借助无线技术取代有线布线方式构成局域网的新手段。WLAN 可提供传统有线局域网的所有功能，是计算机网络与无线通信技术相结合的产物。目前，WLAN 领域主要是 IEEE 802.11x 标准系列，其中应用最为广泛的是 IEEE 802.11b。

无线城域网是一种有效作用距离比 WLAN 更远的宽带无线接入网络，通常用于城市范围内的业务点和信息汇聚点之间的信息交流和网际接入。有效覆盖区域为 2～10km，最大可达 30km，数据传输率最快可达 70Mb/s，目前的主要技术标准是 IEEE 802.16 系列。

无线广域网(Wireless WAN，WWAN)主要用于满足一个城市范围的信息交流的无线接入需求。IEEE 802.20 和 3G 蜂窝移动通信系统是 WWAN 的主要标准。

2. 无线局域网的扩频技术

无线局域网采用电磁波作为载体传送数据信息，使用的模式主要是窄带和扩频。目前，无线局域网的数据传输通常采用无线扩频技术(Spread Spectrum Technology，SST)。常见的扩频技术包括两种，即跳频扩频(Frequency-Hopping Spread Spectrum，FHSS)和直接序列扩频(Direct Sequence Spread Spectrum，DSSS)，它们都工作在 ISM 频段(Industrial Scientific Medical Band，ISM)上。

3. 无线局域网的拓扑结构

无线局域网分为对等网络和结构化网络两种拓扑结构。

对等网络(Peer to Peer)用于一台计算机(无线工作站)和另一台或多台计算机(其他无线工作站)之间的直接通信，该网络无法接入有线网络中，只能独立使用。对等网络中的一个节点必须能“看”到网络中的其他节点；否则就认为网络中断。因此，对等网络只适用于少数用户的组网环境，并且距离足够近。

结构化网络(Infrastructure)由无线访问点(Access Point，AP)、无线工作站(Station，STA)以及分布式系统(DSS)构成，覆盖的区域分为基本服务区(Basic Service Set，BSS)和扩展服务区(Extended Service Set，ESS)。

4. 无线局域网的主要工作过程

无线局域网的主要工作过程包括扫频、关联、重关联和漫游。

5. 无线局域网的访问控制方式

IEEE 802.11b 标准的无线局域网使用的是带冲突避免的载波侦听多路访问方法(CSMA/CA)。

### 1.2.1.3　10Mb/s 以太网

10Mb/s 以太网一般指速率不大于 10Mb/s 的低速以太网。根据传输介质的不同，10Mb/s 以太网大致有 4 个标准，各个标准的 MAC 子层媒体访问控制方法和帧结构以及物理层的编码方法(曼彻斯特编码)均是相同的，不同的是传输媒体和物理层的收发器及媒体连接方式。按照技术出现的时间顺序，这 4 个标准依次如下。

1. 粗缆以太网(10Base-5)

10Base-5 采用 RG-11 型粗同轴电缆为传输介质，其阻抗为 50Ω，直径为 0.4in。在 10Base-5 中，每个计算机节点都通过网卡(AUI 接口)、收发器电缆(AUI Cable)和“收发器”与总线相连，如图 1-1 所示。

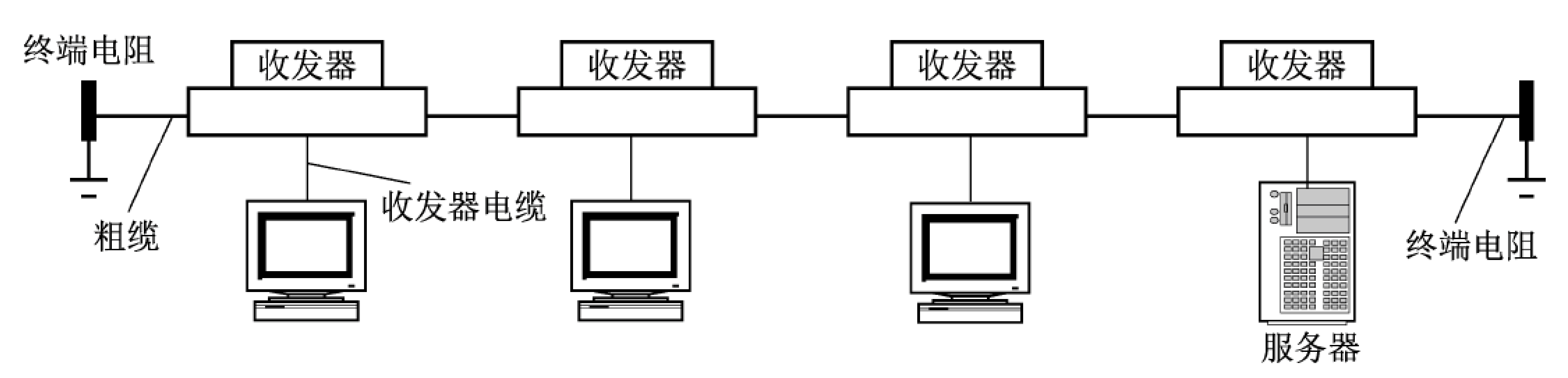



图 1-1　10Base-5 网络结构

10Base-5 代表的具体意思是：工作速率为 10Mb/s，采用基带信号，每一个网段最长为 500m。

通常在标准以太网网络接口板上提供一个 15 针的 AUI(DIX)接口，收发器电缆采用 78Ω 的 6 对屏蔽双绞线电缆(STP)，将收发器与 PC 网卡连接，粗同轴电缆两端接上 50Ω的终端匹配器(也称为端接器)，其中之一必须接地，这就构成了网络段，每段最远距离为 500m。一个粗缆以太网最多可以有 5 段。电缆最大距离是 2.5km，工作站之间的最小距离为 2.5m，收发器电缆的最长距离为 50m。

1) 硬件基本配置

(1) 网卡。联网的每个节点都需要一块带有 15 针 AUI(DIX)接口的 10Mb/s 网卡。

(2) 收发器。粗缆以太网的每个节点需要通过一个安装在总线同轴电缆上的外部收发器(带有 15 针的 AUI 接口)连入网内。

(3) 收发器同轴电缆(AUI 电缆)。它用于节点中网卡与收发器的连接。

(4) 电缆系统。RG-11 型 50Ω粗同轴电缆，终端电阻安装在电缆的两端，以防止信号的反射，其中之一必须接地。

(5) 中继器。它主要用来扩展作为总线的同轴电缆长度和工作站(节点)个数。

2) 主要技术参数

在粗缆以太网中，不使用中继器时每段粗缆的最大距离为 500m。如果使用中继器，应遵循 5-4-3 规则，即一个粗缆以太网中最多允许使用 4 个中继器，连接 5 段最大长度为 500m 的粗同轴电缆；而 5 段中只有 3 段可以连接工作节点，其余两段只能用于扩展网络距离。使用中继器后的粗缆以太网的最大长度不能超过 2.5km；由于每个以太网段中连入的节点数最多为 100 个，且最多可以有 3 个网段连接工作节点，因此，最多有 300 个工作节点；两个相邻的收发器之间的最小距离为 2.5m，收发器电缆的最大长度为 50m。

3) 特点

(1) 优点。可靠性高，抗干扰能力强，作用距离长。

(2) 缺点。粗缆较贵，而且要求每个工作站都配置一个外部收发器和收发器电缆，因而成本较高、网络投资较大。

4) 主要技术规范

(1) 拓扑结构：总线。

(2) 介质访问控制方法：CSMA/CD。

(3) 网络类型：RG-11 型 50Ω粗同轴电缆。

(4) 传输速度：10Mb/s。

(5) 最大网络节点数目：300 个。

(6) 每段最大节点数目：100 个。

(7) 最大网段数目：5 个，最多使用 4 个中继器，其中 3 个网段可连接工作节点。

(8) 节点间的最小距离：2.5m。

(9) 最大网络长度：2.5km。

(10) 最大网段长度：500m。

2. 细缆以太网(10Base-2)

10Base-2 使用 RG-58 型细缆、BNC-T 型连接器，以线性总线进行布线。10Base-2 将原来 10Base-5 的收发器功能移植到网卡上，因此，使得网络的组建更简单，性价比也比 10Base-5 高，然而，却也因此限制了信号能够传送的最大距离。其结构如图 1-2 所示。

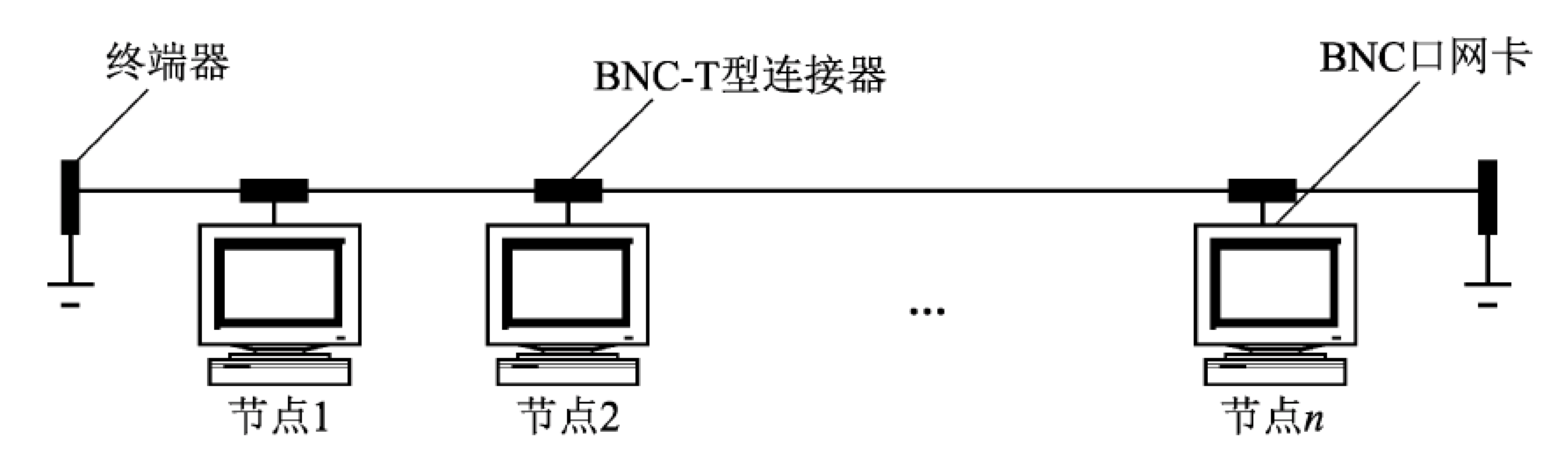



图 1-2 10Base-2 网络结构

10Base-2 代表的具体意思是：工作速率为 10Mb/s，采用基带信号，每一个网段最长约为 200m。

一个细缆以太网的“单段”最大长度为 185m，最多可使用 4 个中继器，即可以有 5 个电缆段，而 5 段中只有 3 段可以连接工作节点，其余两段只能用于扩展网络距离。电缆总长度最大为 925m。一个网段中节点的最多数目为 30 个，因此，最多可以有 90 个工作节点。

两个相邻的 BNC-T 型连接器的最小距离为 0.5m，每段的两端都必须安装一个 50Ω终端匹配器，并且其中一端应接地。网卡提供 BNC 接口，同轴细缆通过 T 形接头与网卡连接，所有 T 形接头必须直接接到工作站 BNC 接口上，中间不得接入任何电缆。

图 1-3 所示为一个使用中继器扩展网络距离的双网段 10Base-2 组网实例。

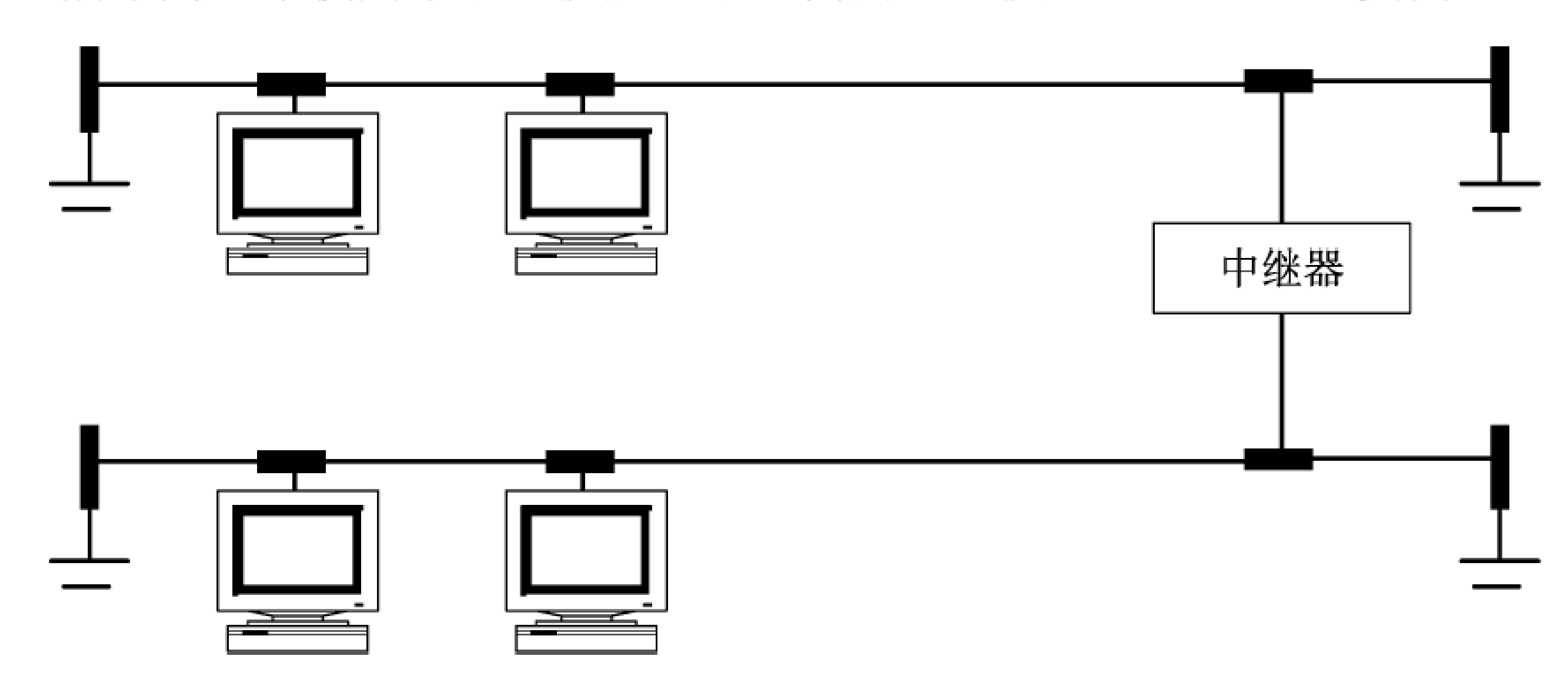



图 1-3　使用中继器连接的双网段 10Base-2 网络结构

1)　硬件基本配置

(1)　网卡：带有 BNC 接口的 10Mb/s 网卡。

(2)　BNC-T 型连接器：细缆以太网中的每个节点通过 BNC-T 型连接器连入网内。

(3)　电缆系统：RG-58 型 50Ω细同轴电缆，终端电阻安装在电缆的两端，防止信号的反射，其中之一必须接地。

(4)　中继器：主要用来扩展作为总线的细缆长度和工作站(节点)个数。

2)　特点

(1)　优点。系统造价低廉，安装容易，具有最短的布线距离。

(2)　缺点。由于缆段中连入多个 BNC-T 型连接器，存在着多个 BNC 型连接头和 BNC-T 型连接器的连接点，因而同轴电缆连接的故障率较高。

3)　技术规范

(1)　拓扑结构：总线。

(2)　介质访问控制方法：CSMA/CD。

(3)　网络类型：RG-58 型 50Ω细同轴电缆。

(4)　传输速度：10Mb/s。

(5)　最大网络节点数目：90 个。

(6)　每段最大节点数目：30 个。

(7)　最大网段数目：5 个，最多使用 4 个中继器，其中 3 个网段可以连接工作节点。

(8)　节点间的最小距离：0.5m。

(9)　最大网络长度：925m。

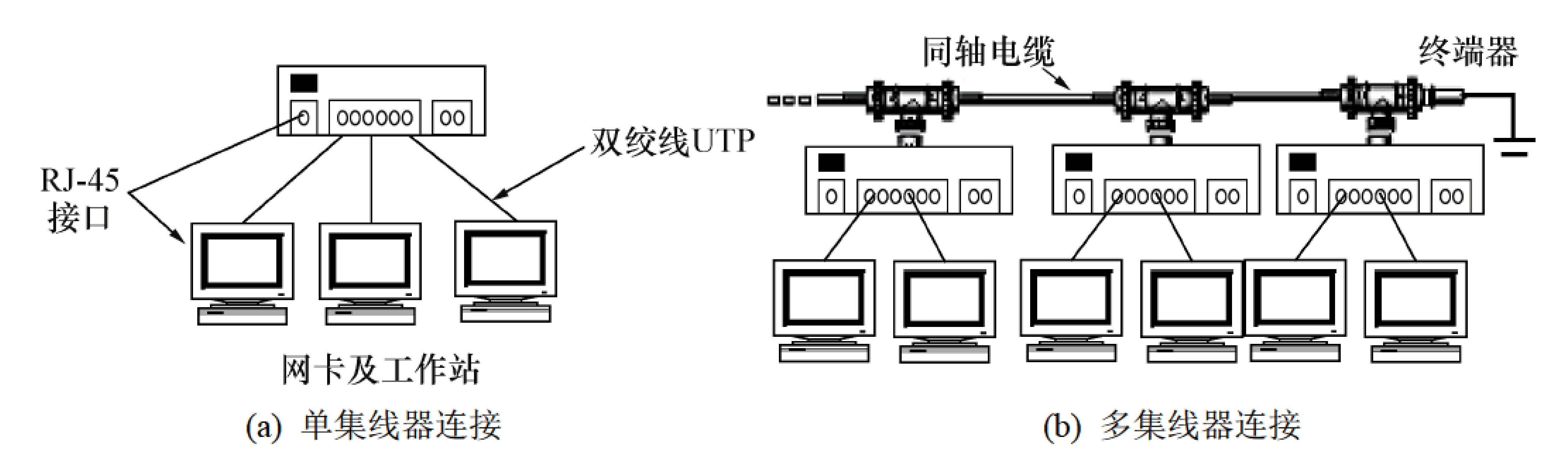
(10) 最大网段长度：185m。

3. 双绞线以太网(10Base-T)

10Base-T 以太网是使用非屏蔽双绞线(UTP)电缆来连接的传输速率为 10Mb/s 的以太网。10Base-T 以太网支持结构化布线系统，需要使用集线器(Hub)构成总线型和星型结合的混合型网络拓扑，具有良好的故障隔离功能，使得网络任一段线路或任一工作站点出现障碍时，均不影响网络上的其他站点，简化了网络故障诊断过程，缩短了故障诊断时间，提高了网络故障检测和冲突控制效率，使局域网难以维护的缺点得以产生根本性改变。加之其组网容易，使得 10Base-T 以太网成为目前使用最广泛的局域网系统。

10Base-T 代表的具体意思是：工作速率为 10Mb/s，采用基带信号，T 表示的是传输媒体双绞线。

单个集线器和多个集线器的 10Base-T 以太网连接如图 1-4 所示。




(a) 单集线器连接　　(b) 多集线器连接

图 1-4　10Base-T 以太网连接

1) 硬件基本配置

(1) 集线器。即 Hub，是双绞线以太网的中心连接设备，有多个 RJ-45 型接口，能支持多个工作站(客户机)入网。Hub 上的 RJ-45(级联或普通)接口还可以与其他 Hub 相连，易于扩展网络。Hub 上的 BNC 向上接口与 BNC-T 型连接器相接时，可以与细缆以太网相连。Hub 上的 AUI 接口可以与粗缆以太网的收发器电缆相连。新型的高速 Hub 上还配有光纤接口，通过此接口可以接入光纤主干线。

(2) 非屏蔽双绞线。10Base-T 网络标准最低采用 3 类 UTP，两端都装有同样的 RJ-45 型接头(水晶头)，每一个工作节点都需要一根双绞线电缆，用来连接工作节点上的网卡与集线器。

(3) 网卡。带有 RJ-45 接口的网卡。

2) 扩展组网方案

使用集线器和双绞线的以太网结构分为单集线器结构、多集线器级联结构、叠加集线器结构。

(1) 多集线器级联(Uplink)结构。

对于规模较大或节点(工作站)数超过单集线器的端口数目，常采用多集线器的连接，这就是集线器的“级联”。级联的目的是为了组成更大规模的网络，级联结构的 10Base-T 网络也遵循 5-4-3 规则，即任一条通路上的两台计算机之间最多不能超过 5 段线，即最多可以串联 4 个集线器；这段线既包括集线器与集线器的连线，也包括集线器到计算机间的连线。注意：3 个集线器能连接设备，两个只能用于级联。网络上连接设备的总数不得超过 1024 台。在级联之前必须首先弄清集线器上的端口类型。

普通集线器提供的端口类型有以下 3 类。

① 用于连接节点(工作站或服务器)的普通 RJ-45 端口。

② 专门用于双绞线以太网集线器的级联端口，即专门用于级联的“出口/入口”或 Uplink 端口。

③ “向上连接端口”。这些端口可以连接粗缆的 AUI 端口或细缆的 BNC 端口，也可以连接光纤端口。

(2) 对应于不同的端口，多集线器结构的级联有以下几种方法。

① 使用“标准线”，通过以太网集线器上专门的 RJ-45 型级联“出/入”端口进行级联。

② 对于没有专门级联“出口/入口”的两个集线器，可以使用“标准线”将一个集线器上边的 Uplink 端口与另一个集线器上边的普通 RJ-45 型端口相连，从而实现多集线器之间的级联。

③ 使用“交叉线”连接两个没有“级联”口的集线器上的普通 RJ-45 接口，也可以实现多集线器的级联。

④ 使用同轴电缆、光纤，通过集线器提供的“向上连接端口”实现级联。

由于 10Base-T 以太网和粗、细缆以太网都属于 IEEE 802.3 规范，因此，互联十分方便。连接时通常采用同轴电缆作为主干网，通过双绞线作为分支网络，这样可以提高干线的可靠性与干扰能力，并可延长传输距离。

利用集线器的“向上连接端口”进行级联，可以扩大局域网覆盖范围。例如，如果使用细缆连接两个集线器，细缆的单根缆段的最大长度为 185m，那么两个 10Base-T 网络中节点的最大距离可达到 385(185+100+100)m。如果使用粗缆连接两个集线器，粗缆的单根缆段的最大长度为 500m，那么网中两节点之间的最大距离可达到 700(500+100+100)m；如果在粗缆或细缆段中配合使用中继器，那么多缆段、多集线器级联系统的覆盖范围还可以更大。

(3) 可叠加集线器以太网结构。

可叠加集线器适用于中小企业联网环境。它由一个基础集线器与多个扩展集线器组成。基础集线器是一个具有网络管理功能的独立集线器。通过基础集线器可以叠加多个扩展集线器，一方面可以增加以太网的节点(工作站)数目；另一方面可以实现对网络中工作节点的网络管理功能。其结构如图 1-5 所示。

3) 特点

(1) 优点。

① 故障检测容易。当某一段线路、工作站或互联的某个 Hub 出现故障时，Hub 会将故障节点自动排除在网络之外，因而保证了剩余部分的正常工作。

② 安装、管理和使用都很简单，适于中小型单位自行组建局域网。

③ 具有成本低、扩展方便、改变网络布局容易等优点。

(2) 缺点。

① 这种结构的最大缺点在于它是一种共享介质的网络，随着网络节点的增加，冲突也会增加，网络的性能也会随之急剧下降。有实验表明，一个单 Hub 的 10Base-T，虽然具有 10Mb/s 的带宽，但是当网络工作节点增至 20 个的时候，其实际的可用带宽将降至原来的 30%～40%。此外，当使用多个 Hub(最多 4 个)级联时，或者是与其他以太网连接之后，

所有网络节点将共享 10Mb/s 的带宽。Hub 所连接的节点越多，每个工作节点得到的带宽就越窄。在高负荷时网络性能将急剧下降，这是组建共享式以太网遇到的最大问题。

② 网络的中央节点的负荷过重，一旦 Hub 出现故障将导致整段或全部网络瘫痪。

③ 双绞线的抗干扰能力弱。

④ 由于每个单段网线只能连接一个工作节点，所以网络通信线路的利用率很低。

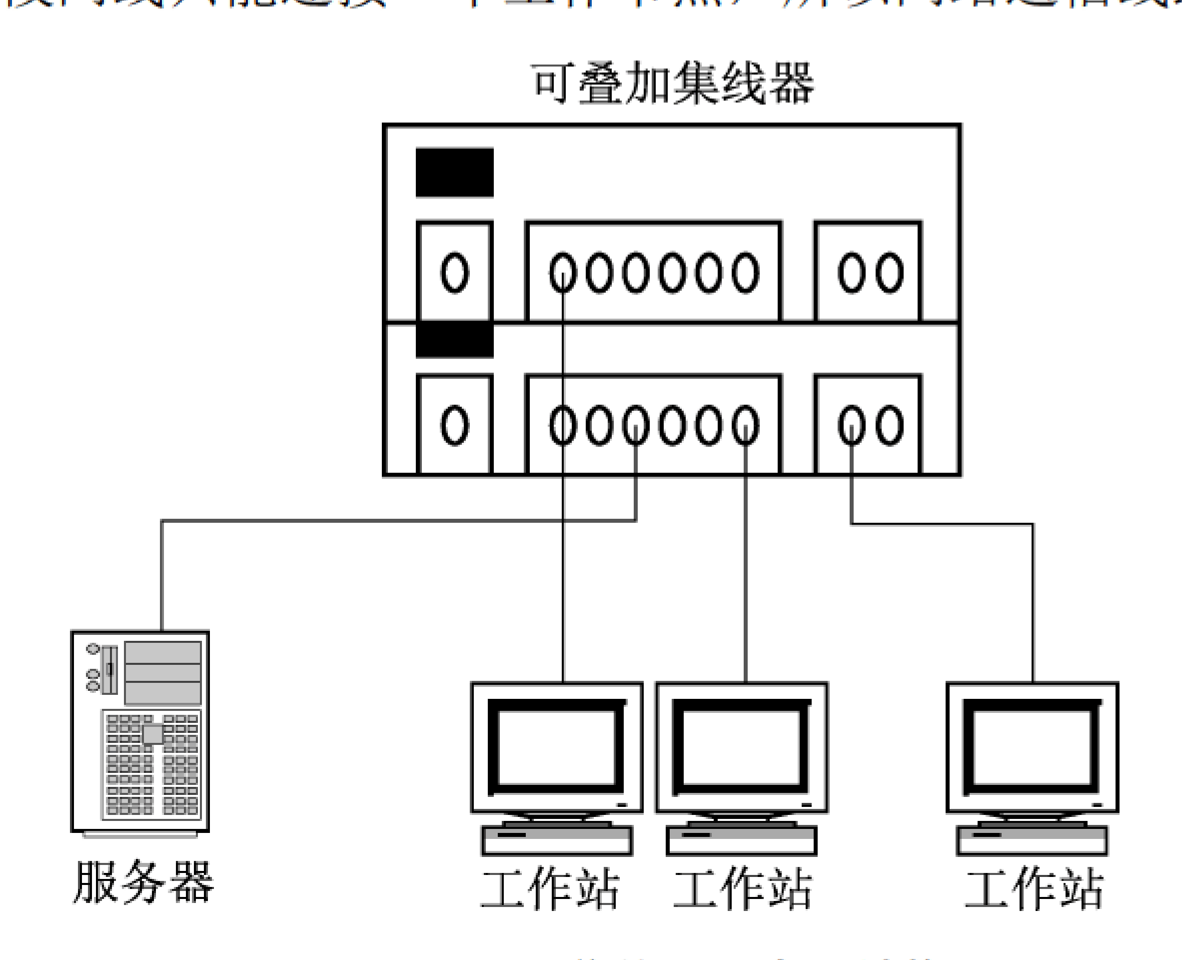



图 1-5　可叠加集线器以太网结构

4) 技术规范

(1) 拓扑结构：由于介质访问控制方法为 CSMA/CD，因此，10Base-T 是逻辑上的总线型拓扑结构、物理上的星型拓扑结构。

(2) 网线类型：3 类、5 类或超 5 类的非屏蔽双绞线。

(3) 传输速度：10Mb/s。

(4) 最大网络节点数目：1024 个。

(5) 每段最大集线器数量：1 个。

(6) 级联的最大集线器数量：4 个。

(7) 最大网络长度：500m。

(8) 最大网段长度：100m。

4. 光纤以太网(10Base-F)

10Base-F 以太网传输媒体采用多模光纤，拓扑结构为星型，所有站点连接到一个支持光纤接口的中心集线器上，每个电缆段的长度不能超过 2km。

10Base-F 以太网设计也遵循 5-4-3 法则，但由于受 CSMA/CD 碰撞域的影响，整个网络的最大跨距为 4km。

10Base-F 代表的具体含义是：工作速率为 10Mb/s，采用基带信号，F 表示的是传输媒体光纤。

#### 1.2.1.4 快速以太网

1. 快速以太网简介

快速以太网是在传统以太网的基础上发展而来的，因此它不仅保持相同的以太网帧格

式，而且还保留了用于以太网的 CSMA/CD 媒体访问控制方式。由于快速以太网的速率比普通以太网提高了 10 倍，所以快速以太网中的网桥、路由器和交换机都与普通以太网不同，它们具有更快的速率和更短的延时。

目前，正式的 100Base-T 标准定义了 3 种物理层规范以支持不同的物理介质，具体如下。

(1) 100Base-TX 用于两对 5 类 UTP 或 1 类 STP。

(2) 100Base-T4 用于四对 3 类、4 类或 5 类 UTP。

(3) 100Base-FX 用于光纤。

其中，100Base-TX 规范描述如何通过 1 类屏蔽双绞线或者 5 类非屏蔽双绞线传送快速以太网帧。5 类 UTP 是目前使用最为广泛的介质，100Base-TX 标准使用其中两对，连接方法和 10Base-T 完全相同，其采用的拓扑结构为星型。这就意味着不必改变布线格局就可直接将 10Base-T 的布线系统移植到 100Base-TX 上。

100Base-T4 规范提出了 100Base-TX 在 3 类 UTP 上传送数据的具体规定，即 100Base-T4 使用四对 3 类、4 类或 5 类 UTP，连接最大距离为 100m。而 10Base-T 只使用两对线，因此老式的 3 类 UTP 布线的 10Base-T 系统必须改变端点上的电缆连线，才能正常运行 100Base-T4。

100Base-FX 是针对光纤提出的物理层规范，它的连线比 100Base-TX 长(450m)，如果采用非标准的全双工模式，连线长度可达 2km，单模光纤传输距离可达 40km。另外，其抗干扰能力也大大优于 UTP 和 STP。

### 2. 100Base-T 组网方法

目前大部分以太网系统都配置一台或多台服务器，在采用以太网/快速以太网交换技术升级组网时，可以将原以太网服务器的网卡更换为快速以太网卡(100Base-TX 网卡)，并利用 5 类 UTP 通过 RJ-45 端子接入 100Mb/s 交换机的 100Mb/s 高速端口上。对于一般工作站，不必更换网卡，可通过原来的共享 Hub 集中连接到 100Mb/s 交换机级联的 10/100Mb/s 交换机的 10Mb/s 端口上，组成 10Mb/s 共享网。对于那些对带宽要求较高的数据库服务器、工作站及打印机等，可单独连接到 10/100Mb/s 交换机的端口上，组成多级交换机的快速以太网，其连接方法如图 1-6 所示。

### 3. 快速以太网的拓扑结构

100Base-T 除了在传输介质、网卡、工作站、Hub 以及服务器硬件组成等方面与 10Base-T 相同外，还保持了 10Base-T 的网络拓扑结构，即所有站点都连接到集线器或交换机上，而集线器与站点间的最大距离仍为 100m。由于 100Base-T 对 MAC 子层的接口有所拓展，因此，快速以太网的拓扑结构形式也有相应的发展。

100Base-T 的拓扑规则如下。

(1) 最大 UTP 电缆长度为 100m。

(2) 在一条链路上，对于 I 类中继器(延时为 0.7μs 以下)，最多只能使用一个，可以构成每段长 100m 的两段链路，即站点到中继器距离为 100m，中继器到交换机距离为 100m。对于 II 类中继器(延时为 0.46μs 以下)，最多使用两个，可有每段长为 100m 的两段链路和 5m 长的中继器间链路，其中站点到第一个中继器(可用集线器)的距离为 100m，集线器与第二个中继器间的距离为 5m，第二个中继器到路由器或交换机的距离为 100m，站点到交换机

的最大距离为 205m。

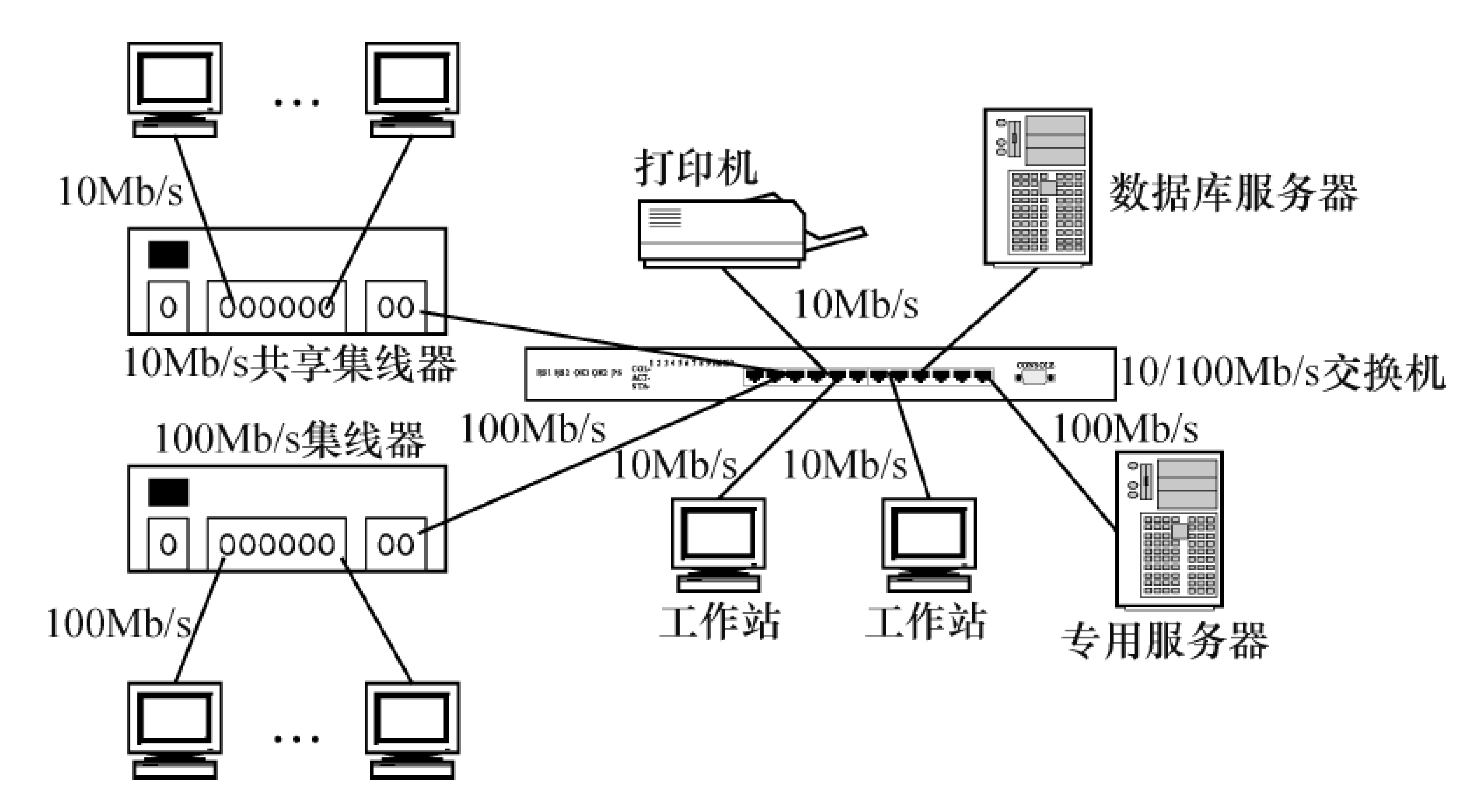



图 1-6　多级交换机快速以太网

(3) 对于光纤作为垂直布线的拓扑结构，纵向只能连接一个中继器(Hub)，各站点到 Hub 的最大距离为 100m，而 Hub 到交换机(或路由器)的垂直向下链路可采用 225m(最大限度)光纤，站点到交换机的最大距离为 325m。

(4) 利用全双工光纤的拓扑结构，通过非标准的 100Base-FX 接口连接，可以使站点(远程)或集线器到路由器或交换机的距离达到 2km。

根据上述规则构成的 100Base-T 拓扑结构如图 1-7 所示。将上述规则进行组合，利用光纤和交换机、网桥、路由器来连接主干设备、网段和工作站，可实现大型企业级和政府级网络。

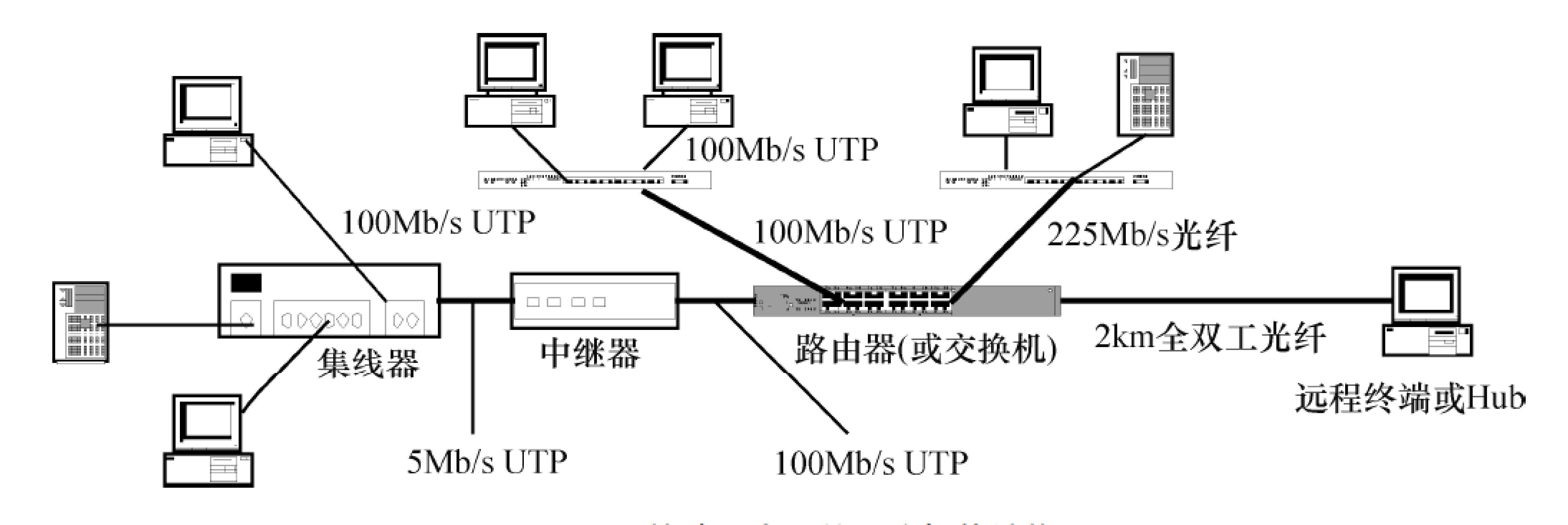



图 1-7　快速以太网的网络拓扑结构

### 1.2.1.5　千兆位以太网

千兆位以太网是 IEEE 802.3 标准的扩展，在保持与以太网和快速以太网设备兼容的同时，提供 1000Mb/s 的数据带宽。千兆位以太网为交换机到交换机和交换机到节点工作站的连接提供了新的全双工操作模式，还为采用中继器和 CSMA/CD 共享连接提供了半双工操作模式。千兆位以太网与 IEEE 802.3 网络采用同样的帧格式、大小以及管理方式。它最初要求使用光纤电缆，但目前在 5 类非屏蔽双绞线电缆中也能很好地实现。

1. 千兆位以太网的分类

千兆位以太网根据传输介质的不同可以分为 4 种，如表 1-1 所示。

表 1-1　千兆位以太网的主要参数

| 千兆位以太网标准 | 传输介质 | 最大传输距离/m | |
|---|---|---|---|
| | | 半双工 | 全双工 |
| 1000Base-SX | 62.5μm MMF | 275 | 300 |
| | 50μm MMF | 330 | 550 |
| 1000Base-LX | MMF | 330 | 550 |
| | SMF | 330 | 5000 |
| 1000Base-CX | 铜质屏蔽双绞线 | 25 | 25 |
| 1000Base-TX | 超 5 类非屏蔽双绞线(4 对) | 100 | 100 |

千兆位以太网标准只允许在媒体段中配置一个中继器，实际上在半双工模式下也只能配置一个中继器，增加一个中继器后铜缆媒体的跨距会增大一倍，而光纤媒体的跨距反而会减少。其系统覆盖范围如下。

- 1000Base-LX/SX：240m。
- 1000Base-CX：50m。
- 1000Base-TX：200m。

2. 以太网向千兆位以太网的升级方法

现有以太网将逐渐向千兆位以太网升级，升级首先在现有的以太网 LAN 骨干网上进行，然后是服务器连接的升级，最终是工作站的升级。这些升级包括以下几个方面。

(1) 交换机到交换机链路的升级。快速以太网交换机或中继器之间的 100Mb/s 链路会被 1000Mb/s 的链路所替代，以提高骨干网交换机之间的通信速度，并支持更多的交换型和共享型快速以太网网段。

(2) 交换机到服务器链路的升级。在交换机和高性能服务器之间实现 1000Mb/s 链路的连接，并要求服务器安装千兆位以太网网卡。

(3) 快速以太网骨干网的升级。带有 10/100Mb/s 端口的快速以太网交换机可以升级支持多路 100/1000Mb/s 端口的千兆位以太网交换机或路由器和集线器(具有千兆位以太网接口和中继器)。这种升级允许服务器通过千兆位以太网网卡直接连接到骨干网上，可增加用户的高带宽应用与服务器的流量。千兆位以太网可以支持更多的网段、带宽和节点。

(4) 高性能工作站的升级。千兆位以太网网卡可将高性能工作站计算机升级到千兆位以太网。这些工作站计算机要连接到千兆位以太网的交换机或中继器上。

3. 千兆位以太网的应用

千兆位以太网可以用于布线间到网络核心的通信，如图 1-8 所示。如需要为个别用户提供 10Mb/s 或 100Mb/s 交换或组交换时，可以通过快速以太网连接，也可以通过千兆位以太网链路连接。为了提高文件服务器的吞吐性能，它的连接也可以通过千兆位以太网进行。

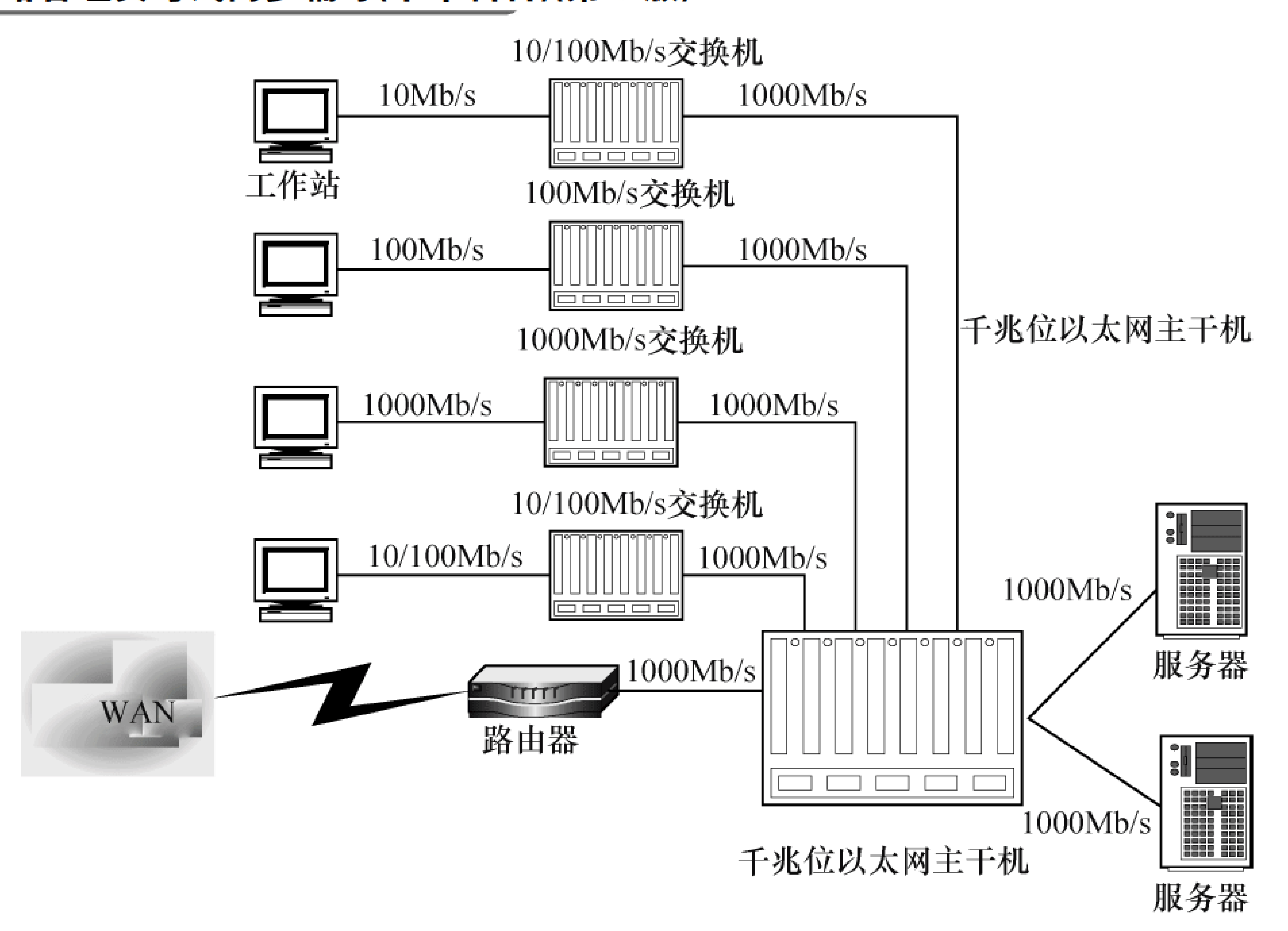



图 1-8　千兆位以太网与多个交换机的连接示意

### 1.2.1.6　万兆位以太网

1. 10Gb/s 以太网

2002 年，IEEE 802.3ae 10Gb/s 以太网标准发布，以太网的发展势头又得到了一次增强。

物理层：IEEE 802.3ae 大体分为两种类型，一种是与传统以太网连接，速率为 10Gb/s 的 LAN PHY；另一种是 SDH/SONET 连接，速率为 9.58464Gb/s 的 WAN PHY。

传输介质层：IEEE 802.3ae 目前支持 9μm 单模光纤、50μm 多模光纤和 62.5μm 多模光纤。

数据链路层：IEEE 802.3ae 目前继承了 IEEE 802.3 以太网的帧格式和最大/最小帧长度，支持多层星型连接、点到点连接及其组合，充分兼容已有应用，不影响上层应用，进而降低了升级风险。与传统的以太网不同，IEEE 802.3 仅支持全双工方式，而不支持单工和半双工方式，不采用 CSMA/CD 机制。IEEE 802.3ae 不支持自协商，可简化故障定位，并提供广域网物理层接口。

2. 40Gb/s 以太网

未来两年内，以太网最高数据传输速率将可望提高至 40Gb/s。Cafiero 称，业内将 40Gb/s 而非 100Gb/s 确定为以太网下一步发展目标的重要原因在于，与 100Gb/s 以太网相比，研发 40Gb/s 以太网在技术上面临的挑战相对较小，更为切实可行。与此同时，Cafiero 还指出，实际上，借助新发布的 Supervisor Engine 720 引擎，Cisco 公司的 Catalyst 6500 旗舰级企业交换平台目前已可以为每一接口卡提供 40Gb/s 的数据传输速率支持。Cafiero 还指出，新型以太网技术成功的关键在于能够推动单位数据传输成本的下降。

### 1.2.1.7　局域网交换技术

1. 共享型以太网

共享型以太网，即在一个逻辑网络上的每一个工作站都处于一个相同的网段上。以太网采用 CSMA/CD 机制，整个系统处在一个碰撞域范围中，系统中每个站点都可能往媒体上发送帧，那么每个站点要占用媒体的概率就是(10Mb/s)/$n$，其中 $n$ 为站点数。这种冲突检测方法保证了只能有一个站点在总线上传输。如果有两个站点试图同时访问总线并传输数据，就意味着“冲突”发生了，两站点都将被告知出错。然后它们都被拒发，并将等待一段时间以备重发。

这种机制就如同许多汽车抢过一座窄桥，当两辆车同时试图上桥时就发生了“冲突”，两辆车都必须退出，然后再重新开始抢行。当汽车较多时这种无序的争抢会极大地降低效率，造成交通拥堵。

网络也是一样，当网络上的用户量较少时，网络上的交通流量会较小，冲突也就较少发生，在这种情况下冲突检测法效果较好；当网络上的交通流量增大时冲突也增多，同时网络的吞吐量也将显著下降；在交通流量很大时，工作站可能会被一而再、再而三地拒发。

2. 交换型以太网

为了解决共享以太网的问题，产生了交换型以太网。用交换机代替 Hub，在交换机上同时存在多个端口间的通道，就是说系统同时存在多个碰撞域，每一个碰撞域的一对端口都独占带宽(一个享有发送带宽，另一个享有接收带宽)，整个系统的带宽与交换机所具有的端口数有关。可以认为，若每个端口为 10Mb/s，则整个系统带宽可达 10Mb/s×$n$，其中 $n$ 为端口数；若 $n$=10，则系统带宽可达 100Mb/s。

3. 全双工以太网

传统的共享型以太网只以半双工模式工作，即网络在同一时间要么发送数据，要么接收数据，而不能同时发送数据和接收数据。全双工以太网与传统半双工以太网技术之间的区别在于：每个端口和交换机背板之间都存在两条逻辑通道。这样每一个端口就可以同时接收和发送帧，不再受 CSMA/CD 的约束，在端口发送帧时不再发生帧的碰撞，已无碰撞域的存在。这样一来，端口之间媒体的长度仅受到数字信号在媒体上传输衰变的影响，而不像传统以太网半双工传输时还要受到碰撞域的约束。其优点是，传输速度加快，比光纤传输介质的传输距离更长。

### 1.2.1.8　局域网设备

计算机网络的组成可分为硬件与软件两大部分：硬件部分包括文件服务器、工作站、网卡、传输介质、接头、网络中的设备、不间断电源系统(UPS)、打印机等；软件部分则包括网络操作系统(如 Windows NT、Linux、Novell、Netware 等)、网络管理系统和应用软件系统。

1. 服务器与工作站

服务器的主要功能是通过网络操作系统控制和协调网络各工作站的运行，处理和响应各工作站同时发送来的各种网络操作要求，提供网络服务。工作站是网络各用户的工作场

所，通常是一台微机或终端。

根据应用类型，网络服务器可分为文件服务器、应用程序服务器、通信服务器等几大类。通常，一个网络至少有一个文件服务器，网络操作系统及其实用程序和共享硬件资源都安装在文件服务器上。

按照网络服务器的设计思想分类，一般把服务器分为 3 种类型：一种是入门级服务器，有时也称为 PC 服务器；另一种是工作组级服务器，在中小企业的业务部门中使用，有时也称为部门级或工作组级服务器；还有一种是企业级服务器，一般对企业的整体网络进行部署。

2. 网卡

网卡(Network Interface Card，NIC)也称为网络适配器，是连接计算机与网络的硬件设备。网卡插在计算机或服务器的扩展槽中，通过网线(如双绞线、同轴电缆或光纤)与网络交换数据、共享资源。在网络中，网卡的任务是双重的：一方面它负责接收网络上传过来的数据包，解包后将数据通过主板上的总线传输给本地计算机；另一方面它将本地计算机上的数据打包后送入网络。

3. 传输介质

1) 同轴电缆

同轴电缆抗干扰性好、频带较宽、数据传输稳定、价格适中、性价比高。同轴电缆中央是一根内导体铜质芯线，外面依次包有绝缘层、网状编织的外导体屏蔽层和塑料保护层。

通常按特性阻抗数值的不同，可将同轴电缆分为 50Ω 基带同轴电缆和 75Ω 宽带同轴电缆。前者用于传输基带数字信号，是早期局域网的主要传输媒体；后者是有线电视系统(CATV)中的标准传输电缆，在这种电缆上传输的信号采用了频分复用的宽带模拟信号。

50Ω 基带同轴电缆可分为粗缆和细缆两类。粗缆用于 10Base-5 以太网，最大干线线段长度为 500m，最大网络干线电缆长度为 2.5km，每条干线段支持的最大节点数为 100 个，收发器之间的最小距离为 1.5m，收发器电缆的最大长度为 50m；细缆用于 10Base-2 以太网，最大干线线段长度为 185m，最大网络干线电缆长度为 925m，每条干线段支持的最大节点数为 30 个，BNC-T 型连接器之间的最小距离为 0.5m。使用基带同轴电缆组网，需要在两端连接 50Ω 的反射电阻，又称为终端匹配器。

2) 双绞线

双绞线是由两条导线按一定扭矩相互绞合在一起的类似于电话线的传输媒体，每根线加绝缘层并用颜色来标记。成对线的扭绞旨在使电磁辐射和外部电磁干扰减到最小。使用双绞线组网时，双绞线与网卡、集线器的接口称 RJ-45，俗称水晶头。

双绞线分为屏蔽双绞线和非屏蔽双绞线，STP 双绞线内部包了一层皱纹状的屏蔽金属物质，并且多了一条接地用的金属铜丝线，因此它的抗干扰性比 UTP 双绞线强，阻抗值通常为 150Ω。对于 UTP 双绞线，其阻抗值通常为 100Ω，每条双绞线最大传输距离为 100m。

双绞线的制作有两种方法：一种是直通线，即双绞线的两个接头都按 568B 线序标准连接；另一种是交叉线，即双绞线的一个接头按 EIA/TIA 568A 线序连接，另一个接头按 EIA/TIA 568B 线序连接。

3)　光纤

光纤是新一代的传输介质，与铜介质相比，它具有一些明显的优势。因为光纤不会向外界辐射电子信号，所以使用光纤介质的网络无论是在安全性、可靠性还是在传输速率等网络性能方面都有了很大的提高。

根据光在光纤中的传输方式，可将光纤分为两种类型，即多模光纤和单模光纤。

4)　无线传输

无线传输主要分为无线电、微波、红外线及可见光几个波段。

无线电微波通信在数据通信中占有重要地位。微波的频率范围为 300MHz～300GHz，但主要使用 2～40GHz 的频率范围。微波通信主要有两种方式，即地面微波接力通信和卫星通信。

### 4.　网络互联设备

常用的网络互联设备有中继器、集线器、网桥、交换机、路由器及网关等。

1)　中继器

中继器(Repeater)是网络物理层的一种介质连接设备，它工作在 ISO/OSI 参考模型的第一层(物理层)。当局域网物理距离超过了允许的范围时，可用中继器将该局域网的范围进行延伸。

2)　集线器

集线器(Hub)从工作原理上看就是一个多端口中继器，起到一个信号分散器的作用，它也工作在 ISO/OSI 参考模型的第一层(物理层)，通过一个端口接收信号，然后再发送到其他所有端口。它是在局域网上广泛使用的网络设备，可以用来将若干台计算机通过双绞线或同轴电缆连接到集线器，从而构建一个局域网。

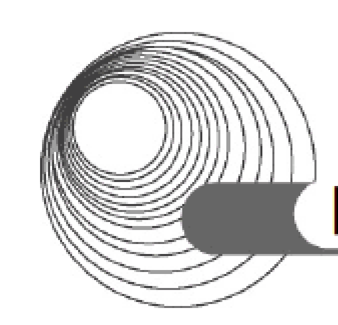
3)　网桥

网桥(Bridge)工作在 ISO/OSI 参考模型的第二层(数据链路层)，与高层协议无关，因此只能连接具有相同高层协议的网络。网桥的工作原理是，通过数据链路层的逻辑链路控制子层选择子网路径，接收完整的 MAC 数据帧并进行差错校验，再根据 MAC 中的源或目的地址决定帧的去向。如果是传给本网段的某一站点，则不予转发；如果目的地址是其他网络段的，则向它连接的所有网络段转发该 MAC 帧。在转发该帧之前，网桥对帧的内容和格式不做修改或仅做少量的修改后发送到物理层，再由物理层的传输介质发送到另外一个子网。

数据链路层连接两个局域网络段指的是网间通信从网桥传送，网内通信被网桥隔离。当网络负载重而导致性能下降时，用网桥可将其分为两个或多个网段，从而最大限度地缓解网络通信繁忙的程度，提高通信效率。

4)　交换机

集线器虽然有多个端口，但同一时间只允许一个端口发送或接收数据；而交换机(Switch)则是采用程控交换机的原理设计的，允许多对端口同时发送或接收数据，每一个端口独占整个带宽，从而提供了一种提高数据传输速率的方法。交换机能够将以太网的速率提高至真正的 10Mb/s 或 100Mb/s。交换机工作在 ISO/OSI 参考模型的第二层(数据链路层)。目前局域网内广泛采用交换机设备。




5) 路由器

当两个不同类型的网络彼此相连时，必须使用路由器(Router)。路由器工作在 ISO/OSI 参考模型的第三层(网络层)，能够提供路由选择、流量控制、协议转换、分组过滤、子网分割等功能。可广泛应用于局域网之间、局域网与广域网之间以及广域网之间的互联。路由器的互联能力强，可以执行复杂的路由选择算法，处理的信息量比网桥多，但处理速度比网桥慢。

路由器在局域网系统中的应用如下。

(1) 局域网互联：连接多个局域网系统并实现局域网系统之间的数据转发。

(2) 局域网隔离：连接多个局域网系统并实现局域网系统之间的数据隔离。

(3) 局域网与广域网互联：局域网通过路由器连接广域网，实现对远程主机的访问。

6) 网关

当连接两个结构完全不同的网络时，必须使用网关(Gateway)。网关又称为协议变换器，它工作于传输层及其以上的层次，是用于在不同网络之间实现协议转换的专用网络通信设备。

网关可以设在服务器、微型机或大型机上。常见的网关有以下 4 种。

(1) 电子邮件网关。可以从一种类型的系统向另一种类型的系统传输数据。

(2) IBM 主机网关。可以在一台个人计算机与 IBM 大型机之间建立和管理通信。

(3) 互联网网关。允许并管理局域网和互联网间的接入，可以限制某些局域网用户访问互联网。

(4) 局域网网关。可以使运行于 OSI 模型不同层上的局域网网段间相互通信。路由器甚至只用一台服务器就可以充当局域网网关。局域网网关也包括远程访问服务器，它允许远程用户通过拨号方式接入局域网。

#### 1.2.1.9 计算机网络接入技术

终端远程接入局域网、局域网与局域网远程互联或局域网接入广域网，这些都必须借助公共传输网络。

公共传输网络的接入技术主要有：公共交换电话网(PSTN)、综合业务数字网(ISDN)、X.25 分组交换网、数字数据网(DDN)、帧中继(FR)、异步传输模式(ATM)、数字用户线路(xDSL)、宽带网接入、HFC 和 Cable Modem 接入技术等。

1. PSTN 接入技术

“拨号接入”就是指通过普通电话线利用调制解调器(Modulator Demodulator，Modem)使用公用交换式电话网(Public Switched Telephone Network，PSTN)来传输数据，普通拨号 Modem 的最高速率为 56kb/s。其接入硬件需要具备一台调制解调器、一条电话线、集线器或交换机、代理服务器(网卡和 Modem 的连接端口)等。代理服务器可安装 WinGate、Sygate 等代理软件，以便代理局域网内的其他计算机访问 Internet。其拓扑结构如图 1-9 所示。代理服务器的串行口 COM 通过串行线与 Modem 相连，网卡通过双绞线与交换机或集线器相连，并根据需求设置该网卡的 IP 地址(私有地址)，如 192.168.1.1，子网掩码为 255.255.255.0，局域网内其他计算机设置的 IP 地址与该服务器的网卡地址位于同一个网段内。

也可使用带有 PSTN 端口的路由器接入 Internet。其拓扑结构如图 1-10 所示。

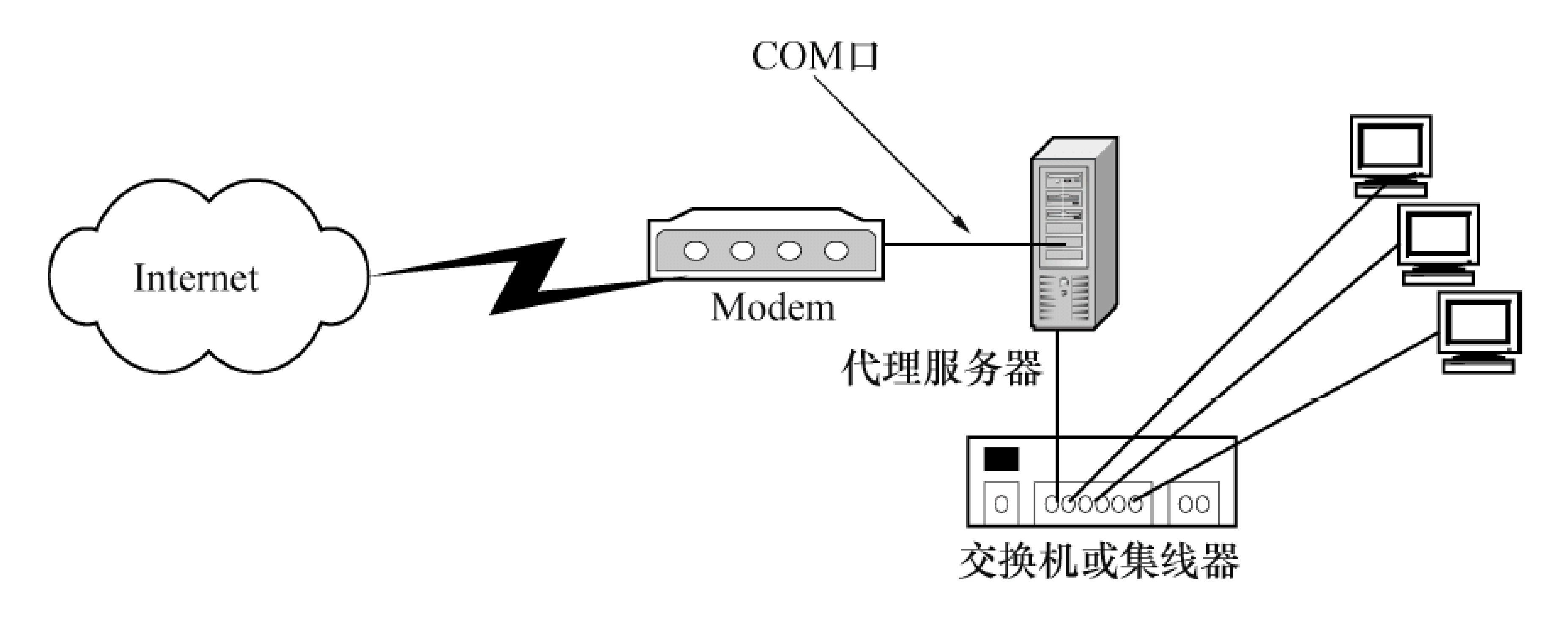



图 1-9　用调制解调器连接 Internet

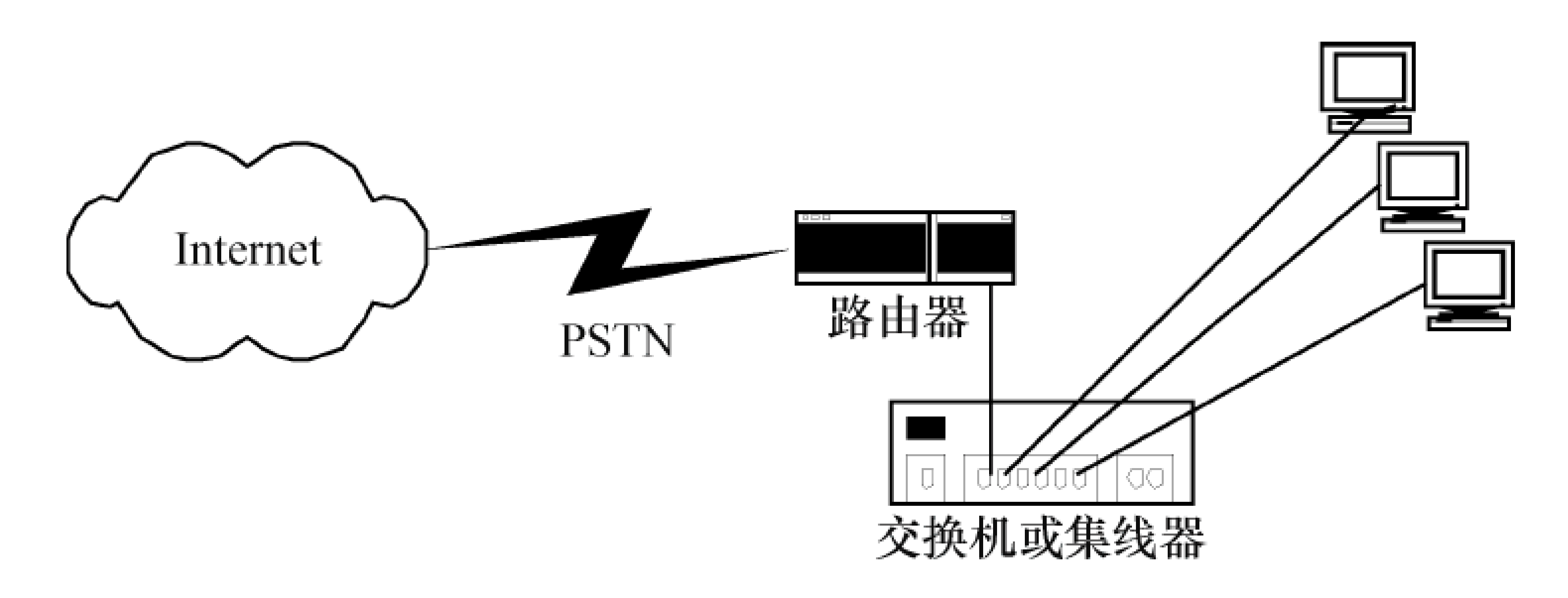



图 1-10　使用路由器接入 Internet

2. ISDN 接入技术

ISDN 是 Integrated Services Digital Network(综合业务数字网)的缩写，能在一根普通电话线上提供语音、数据、图像等综合性业务。ISDN 在一对普通的电话用户线路上，提供两个双向的 64kb/s 的 B 通道和一个 16kb/s 的 D 通道。B 通道是承载通道，可以传送语音和数据。两个 B 通道既可以单独使用，也可以捆绑起来传送数据，都可达到 128kb/s 的速率。ISDN 可连接 8 台终端或电话，有两台终端(如一部电话、一台计算机或一台数据终端)可以同时使用。对于用户而言，同样的一对普通电话线原来只能接一部电话机，而申请了 ISDN 后，通过一个称为 NT 的转换盒，就可以同时使用数个终端。在一根普通电话线上，可以提供以 64kb/s 速率为基础并可达到 128kb/s 上网速度的数字连接。

局域网用户可通过 ISDN 专线接入 Internet，其拓扑结构如图 1-11 所示。所需的硬件设备有 NT1、ISDN 专线、交换机或集线器、代理服务器(ISDN 卡和网卡)等。代理服务器可安装 WinGate、Sygate 等代理软件，以便代理局域网内的其他计算机访问 Internet。

局域网用户也可采用 ISDN 路由器接入 Internet，其拓扑结构如图 1-12 所示。

3. ADSL 接入技术

ADSL 是英文 Asymmetrical Digital Subscriber Loop(非对称数字用户环路)的缩写，ADSL 技术是运行在原有普通电话线上的一种新的高速宽带技术，它利用现有的一对电话铜线，为用户提供上、下行非对称的传输速率(带宽)。非对称主要体现在上行速率(最高 640kb/s)和下行速率(最高 8Mb/s)的非对称性上。上行(从用户到网络)为低速的传输，可达 640kb/s；下行(从网络到用户)为高速传输，可达 8Mb/s。在不影响原有语音信号的基础上，扩展了已有电话线路的功能。

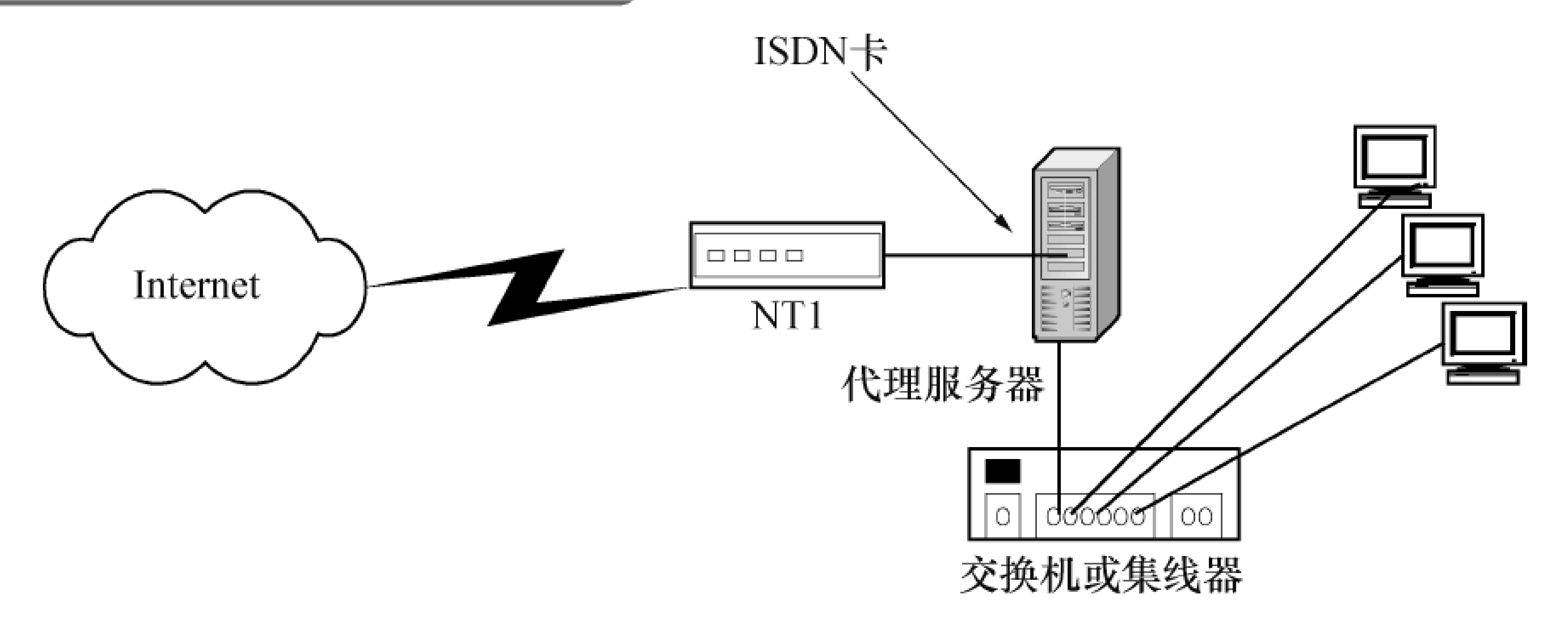



图 1-11　局域网使用 ISDN 专线接入 Internet

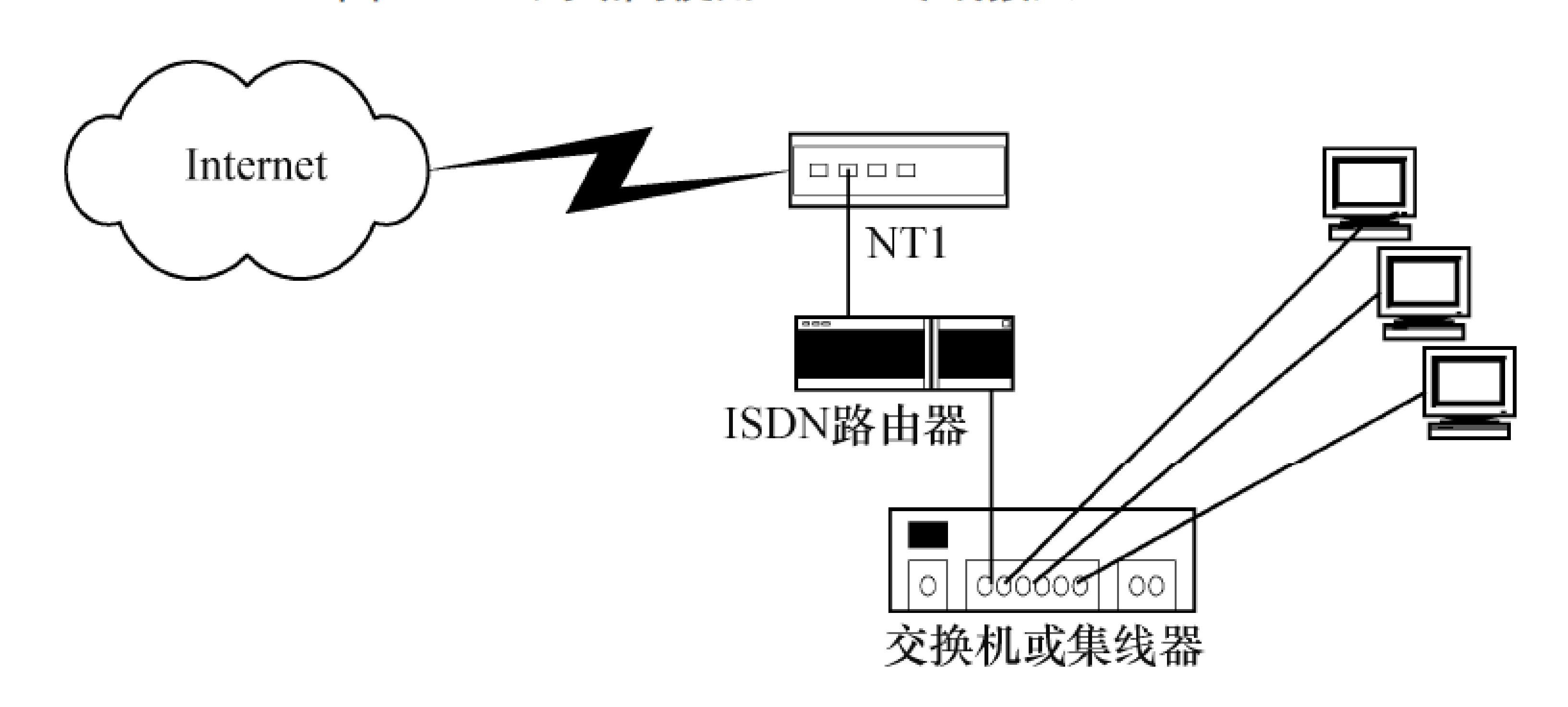



图 1-12　局域网使用 ISDN 路由器接入 Internet

局域网用户可通过 ADSL 接入 Internet，其拓扑结构如图 1-13 所示。所需的硬件设备有语音/数据分离器、ADSL 专线、交换机或集线器、代理服务器(两块网卡)等。代理服务器上连接 ADSL Modem 的那一块网卡设置电信公司提供的 IP 地址、子网掩码、DNS、网关等参数，内网可设置私有地址，并安装代理服务软件，以便代理局域网内的其他计算机访问 Internet。

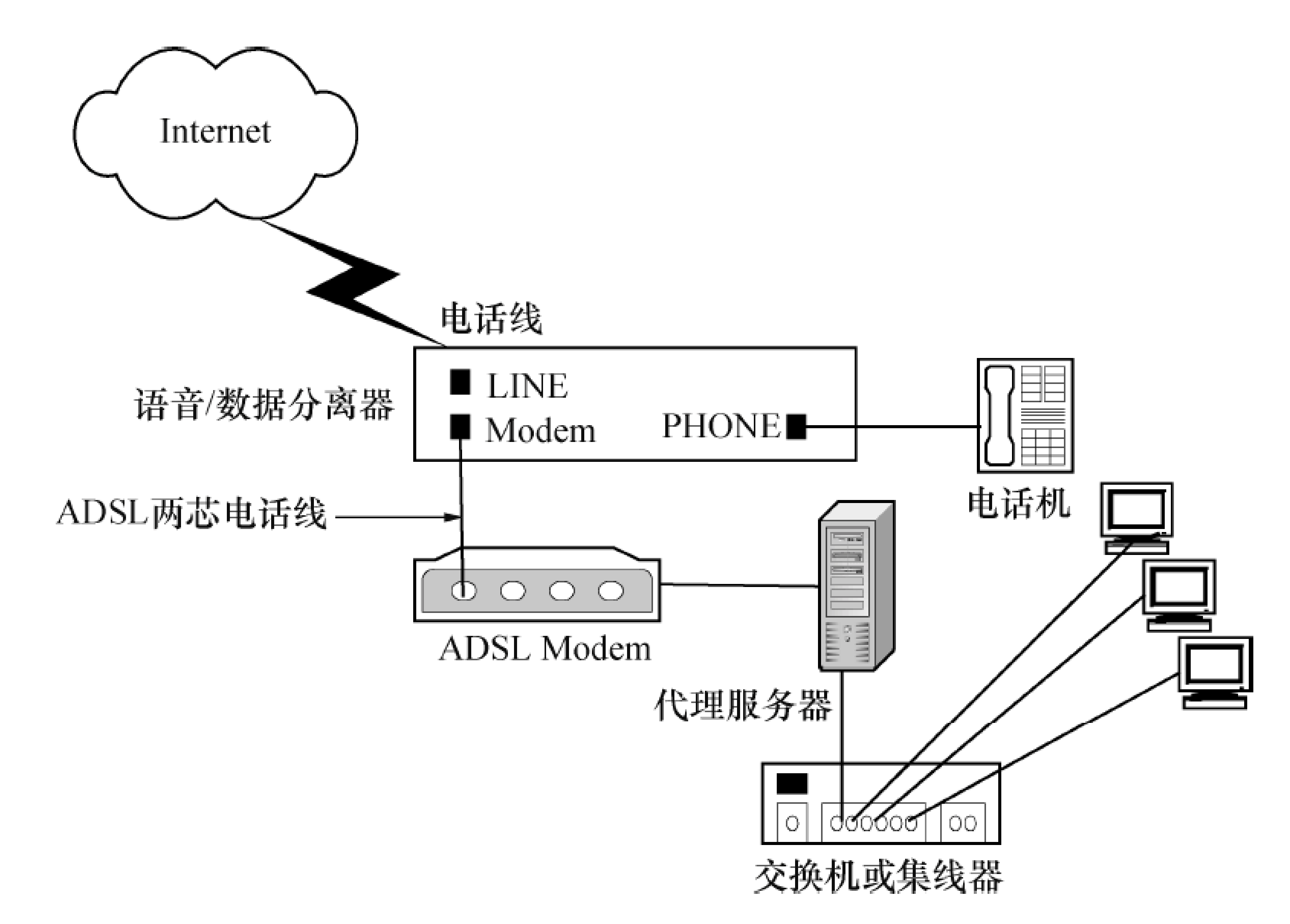



图 1-13　局域网用户使用 ADSL 接入 Internet

局域网用户也可利用 ADSL 路由器接入 Internet，其拓扑结构如图 1-14 所示。

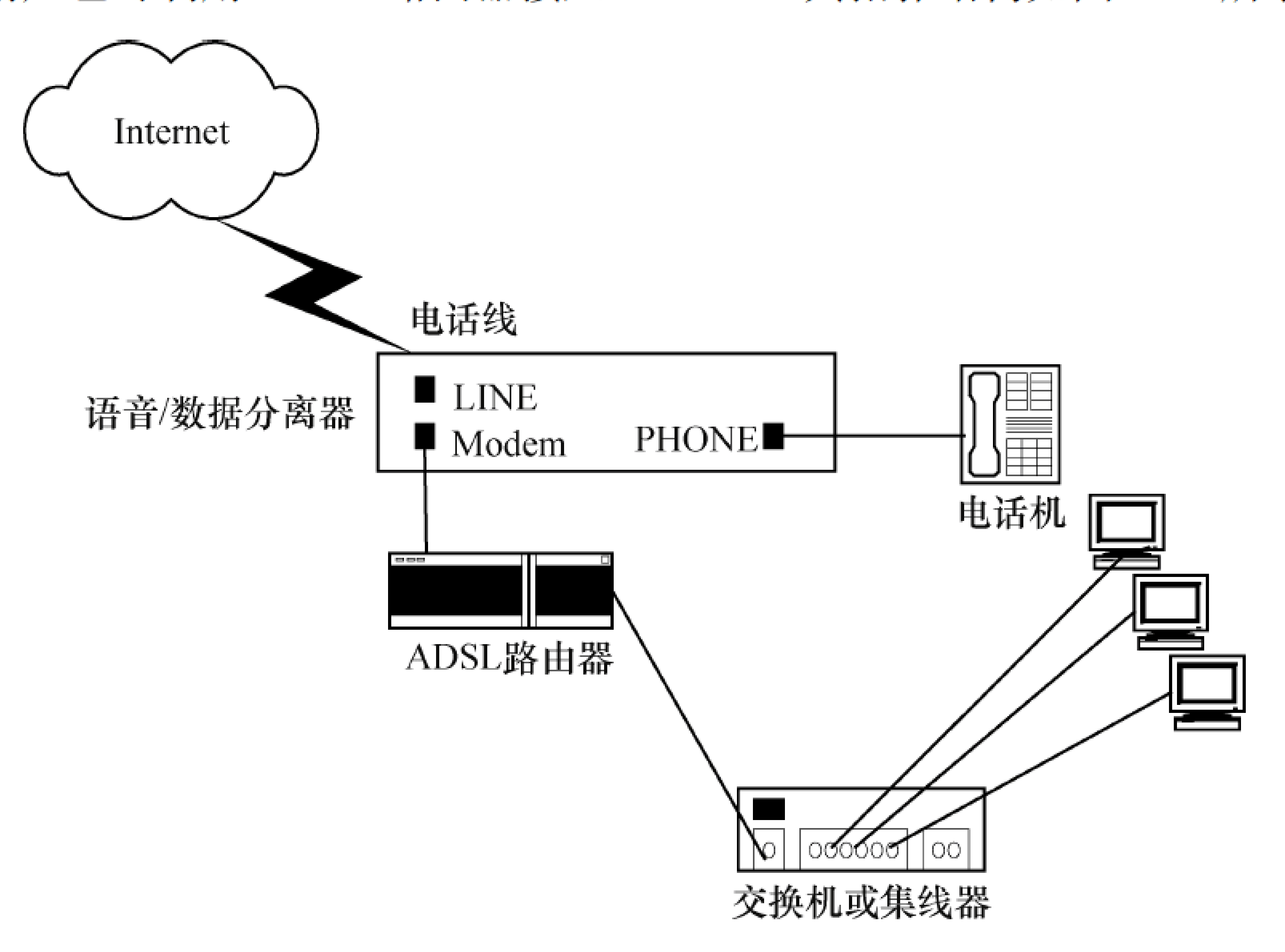



图 1-14　局域网使用 ADSL 路由器接入 Internet

4. 宽带网接入技术

宽带网也称为“IP 城域网”，它是在城市范围内以多种传输介质为基础，采用 TCP/IP 协议，通过路由器组网，实现 IP 数据包的路由和交换传输。

IP 城域网的接入方式目前一般分为 LAN 接入(用网线)和 FTTX 接入(用光纤)。LAN 接入是指从城域网的节点经过交换机和集线器将网线接入到用户家中。FTTX 接入是指光纤直接接入到用户家中，即光纤到户(FTTH)或光纤到桌面(FTTD)，它是未来宽带网络发展的方向。

宽带 IP 网以光纤通信为基础，以成熟的 IP 技术为核心，采用路由器和交换机等设备组网，可为用户提供 10Mb/s、100Mb/s、1000Mb/s 等几种可选接入速率。其速率是目前电话拨号上网的 170 多倍。

宽带 IP 网的建设目标是铺设光纤到小区，到大楼，最终以光纤到户为目标。目前一般采用光纤加局域网的方式实现群体用户接入宽带网络。其拓扑结构如图 1-15 所示。

5. HFC 和 Cable Modem 接入技术

HFC 网是光纤同轴电缆混合网，它是一种新型的宽带网络，采用光纤到服务区，而在进入用户的“最后 1 千米”采用同轴电缆，最常见的是有线电视网络。HFC 网络大部分采用传统的高速局域网技术，而 Cable Modem 是其中最重要的组成部分。

Cable Modem 可以译为电缆调制解调器或线缆调制解调器，它是一种将数据终端设备连接到有线电视网(CATV)，以使用户能够进行数据通信访问 Internet 等信息资源的设备。

6. 数据通信网接入技术

局域网用户还可以通过 DDN 网、X.25 网、帧中继网、ATM 网接入 Internet，其核心设备是路由器等网络终端接入设备。其拓扑结构如图 1-16 所示。

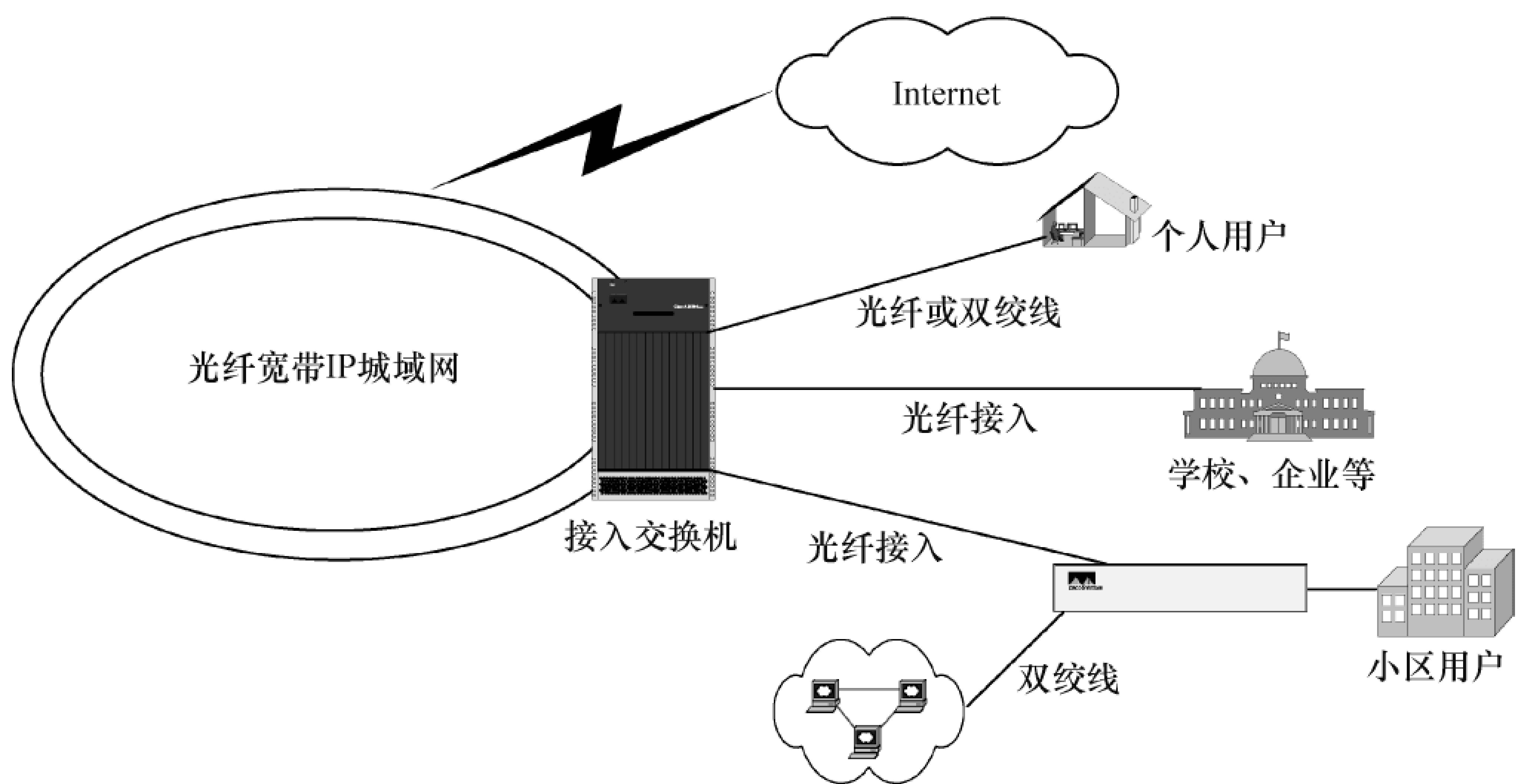



图 1-15　局域网宽带 IP 接入 Internet

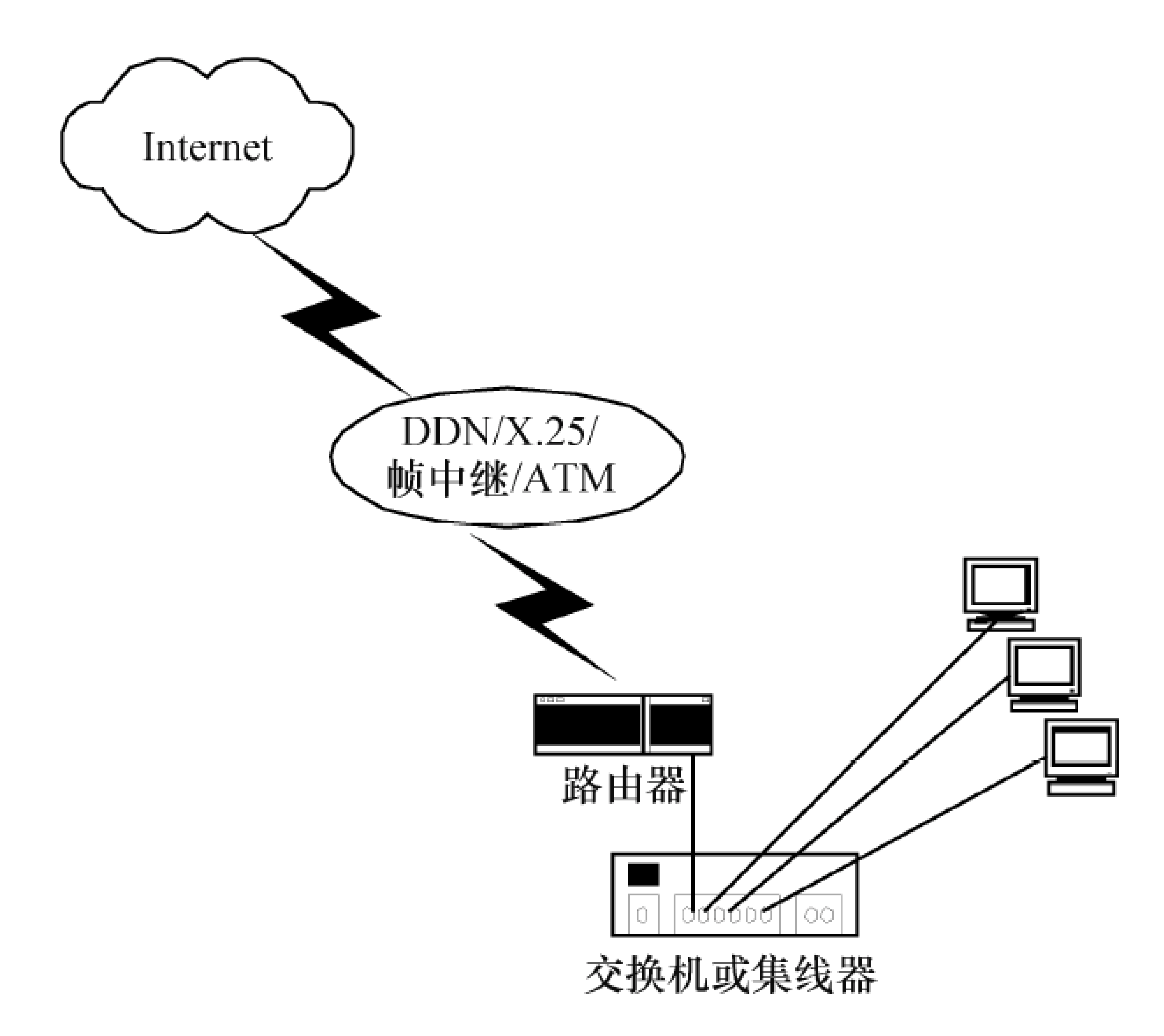



图 1-16　局域网使用数据通信网接入 Internet

1)　X.25 分组交换网

X.25 是 CCITT 制定的在公用数据网上供分组型终端使用的，数据终端设备(DTE)与数据通信设备(DCE)之间的接口建议。它只是一个以虚电路服务为基础的对公用分组交换网接口的规格说明。它动态地对用户传输的信息流分配带宽，能够有效地解决突发性、大信息流的传输问题，分组交换网络同时可以对传输的信息进行加密有效的差错控制。

X.25 一般只用于要求传输费用少，而远程传输速率要求又不高的广域网环境。其速率为 9600b/s～64kb/s。

2)　数字数据网

数字数据网(DDN)是利用数字通道提供半永久性连接电路，向用户提供端到端的中高速率、高质量的数字专用电路，全程实现数字信号透明传输的数据传输网。DDN 网通常由 4

部分组成，包括本地传输系统、复用与交叉连接系统、局间传输与同步系统和网络管理系统等。DDN 干线主要采用光缆、数字微波与卫星信道，所提供的信道是非交换型的半永久电路，通常由电信部门在用户申请时设定，修改并非经常性的。

DDN 采用脉冲编码调制(PCM)的数字中继方式，传输距离远，具有传输速度快、质量好、性能稳定和带宽利用率高等优点。其速率可达 2Mb/s。

3)　帧中继

帧中继是为了克服 X.25 的缺点，提高性能而发展起来的一种高速分组交换与传输技术。它是一种减少节点处理时间的技术。帧中继认为帧的传送基本上不会出错，因此每个节点只要一知道帧的目的地址就立即转发，大大减少了帧在每一个节点的时延，比传统 X.25 的处理时间少一个数量级。

帧中继的设计目标主要是针对局域网之间的互联，它以面向连接的方式、合理的数据传输率和低廉的价格提供数据通信服务。帧中继的主要思想是“虚拟租用线路”。帧中继采用帧作为数据传送单元，网络的带宽根据用户帧传输的需要，可以采用统计复用的方式动态分配，可以充分复用网络资源，从而提高了中继带宽的利用率，尤其对突发信息的适应性比较强。帧中继用户的接入速率为 64kb/s～2Mb/s。

4)　异步传输模式(ATM)

ATM 是 Asynchronous Time division multiplexing 的缩写，译为“异步传输模式”，它是以高速分组传送模式为主，综合电路传输模式优点的一种宽带传输模式。

ATM 系统使用异步时分复用技术的快速分组交换方式，它将信息流分割成固定长度的 ATM 信元，能比较容易地实现各种信息流混合在一起的多媒体通信，能根据业务类型、传输速率等要求动态分配有效容量，对高速信息元传输频次高，对低速信息元传输频次低。因此 ATM 能采用单一的交换方式，支持从窄带语音、数据传输到高清晰度电视(High Definition TeleVision，HDTV)等范围极广的各种业务。

ATM 信元是固定长度的分组，并使用空闲信元来填充信道，从而使信道被分为等长的时间小段。每个信元共有 53 个字节，分为两个部分。前面 5 个字节为信头，主要完成寻址的功能；后面的 48 个字节为信息段，用来装载来自不同用户、不同业务的信息。ATM 接入的速率可达 155～622Mb/s。

## 1.2.2　典型例题分析

**例 1**　目前局域网广泛采用以太网技术。局域网互联时通常采用中继器、集线器、网桥、交换机、路由器、网关等设备，请简要回答下列问题。

**【问题 1】**以太网的标准是什么？

**【问题 2】**中继器、集线器、网桥、交换机、路由器、网关分别工作在 ISO/OSI 参考模型的哪一层？

**【问题 3】**简述路由器的特点。

**分析：**

**【问题 1】**是考查以太网的概念，要求考生对以太网的标准有所了解，属于识记层次，较容易。

**【问题2】**考查局域网互联设备工作在ISO/OSI参考模型的哪一层。中继器是网络物理层的一种介质连接设备，它工作在ISO/OSI参考模型的第一层(物理层)。当局域网物理距离超过了允许的范围时，可用中继器将该局域网的范围进行延伸。集线器从工作原理上看就是一个多端口中继器，它起到一个信号分散器的作用，它也工作在ISO/OSI参考模型的第一层(物理层)，它通过一个端口接收信号，然后再发送到其他所有端口。网桥工作在ISO/OSI参考模型的第二层(数据链路层)，负责接收和转发数据帧，并对数据帧进行管理。交换机从工作原理上看就是一个多端口网桥，它利用存储转发和过滤技术来分割网段，使局域网整体带宽得到成倍提高。路由器工作在ISO/OSI参考模型的第三层(网络层)，它能够在复杂网络中为网络数据的传输自动进行路径选择。网关工作在ISO/OSI参考模型的传输层及其以上的层次，用于在不同网络之间实现协议转换的专用网络通信设备。

**【问题3】**考查路由器的特点。

**答案：**

**【问题1】**以太网的标准是IEEE 802.3。

**【问题2】**中继器工作在ISO/OSI参考模型的第一层，集线器工作在ISO/OSI参考模型的第一层，网桥工作在ISO/OSI参考模型的第二层，交换机工作在ISO/OSI参考模型的第二层，路由器工作在ISO/OSI参考模型的第三层，网关工作在ISO/OSI参考模型的传输层及其以上的层次。

**【问题3】**路由器的特点如下。

(1) 更强的异种网络互联能力。路由器不仅能实现不同类型的局域网互联，而且可以用于局域网与广域网、广域网与广域网的互联，同时它还提供不同网络地址格式的转换功能。

(2) 有较好的拥挤控制能力。路由器具有各种解决拥挤的方法，而网桥只能通过加大缓存来局部解决拥挤问题，同时路由器可以隔离广播信息，避免出现广播风暴。

(3) 具有防火墙功能。路由器通常有多种隔离信息包的方法，从而进一步加强网络的安全保密性，防止网络系统和系统内的数据遭到攻击和破坏。

(4) 便于网络管理和维护。路由器连接的各个网络仍是独立的子网，便于各自管理和维护。并且，通过路由器提供的网管功能，可以随时对各子网的工作状况进行监视和控制，及时发现和解决可能出现的问题。

例2　阅读以下说明，回答问题。

**【说明】**

图1-17是某办公局域网的拓扑结构，采用8口Hub将客户机、打印机及服务器相连，形成一个小型的办公网络。

**【问题1】**该网络采用的媒体访问控制技术是什么？

**【问题2】**局域网的主要网络拓扑有哪些？图1-17采用了哪种网络拓扑?

**【问题3】**Hub与服务器、客户机之间采用什么传输介质？

**分析：**

**【问题1】**考查共享型以太网的概念。用Hub组建的以太网为共享型以太网，采用CSMA/CD媒体访问控制技术是它的特征。

**【问题2】**考查局域网的拓扑结构分类。局域网的拓扑结构通常分为3种，分别是总线

型拓扑结构、星型拓扑结构和环型拓扑结构。总线型结构使用同一媒体或电缆连接所有端用户，也就是说，连接端用户的物理媒体由所有设备共享。星型结构存在着中心节点，每个节点通过点对点的方式与中心节点相连，任何两个节点之间的通信都要通过中心节点来转接。环型结构在 LAN 中使用较多。这种结构的传输媒体从一个端用户到另一个端用户，直到将所有端用户连成环形。

**【问题 3】**考查局域网采用的传输媒体。在 Hub 组建的以太网中，局域网采用两端都装有同样的 RJ-45 型接头(水晶头)，每一个工作节点都需要一根双绞线电缆，用来连接工作节点上的网卡与集线器。

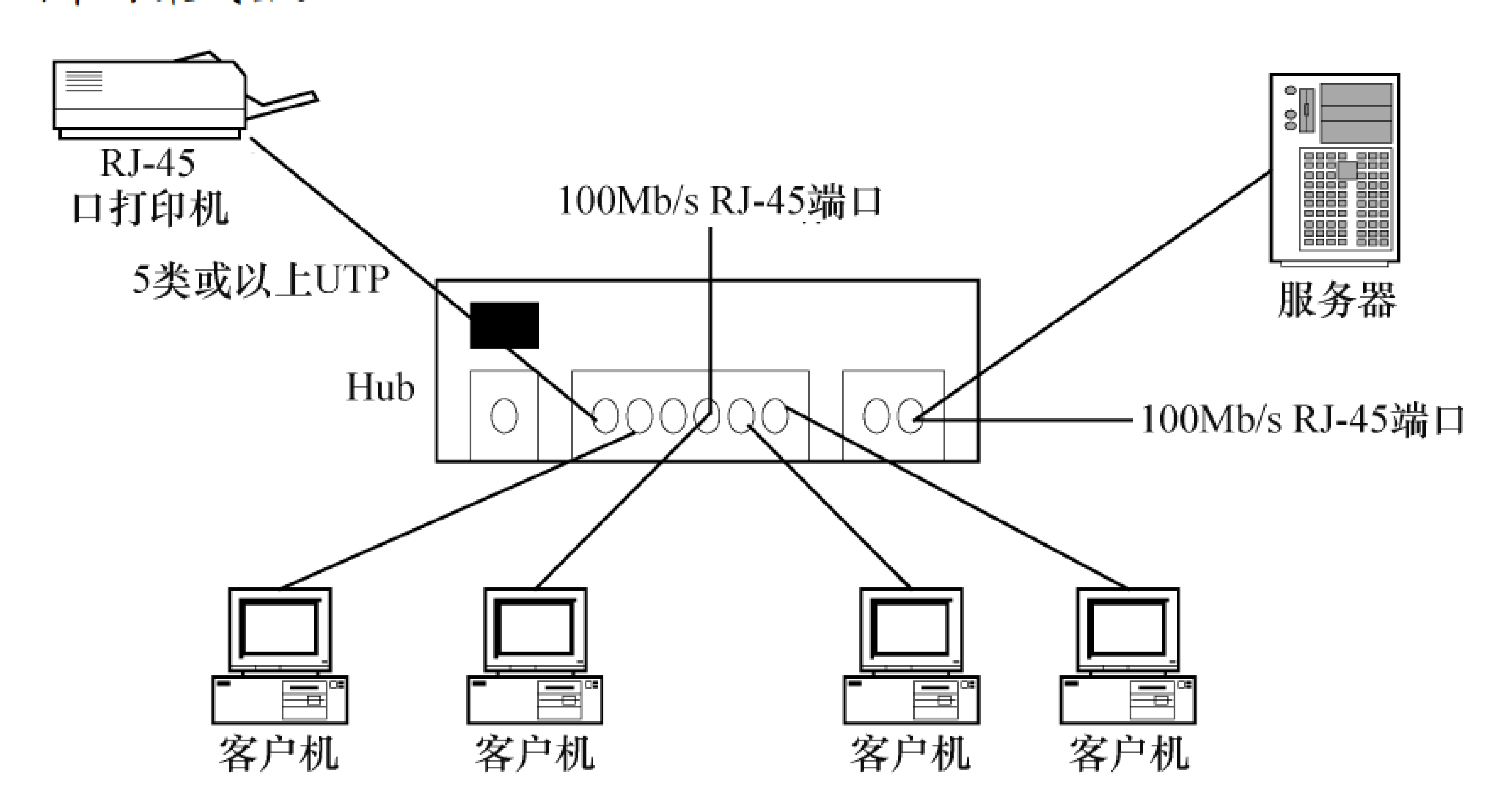



图 1-17　某办公局域网拓扑结构

**答案：**

**【问题 1】**CSMA/CD。

**【问题 2】**局域网在网络拓扑上主要采用了环型、星型和总线型结构。图 1-17 中采用的是星型拓扑结构。

**【问题 3】**双绞线。

例 3　简要回答有关局域网传输媒体的问题。

**【问题 1】**局域网的传输媒体包括哪些种类？

**【问题 2】**目前局域网上常用哪几种传输媒体？

**【问题 3】**目前局域网上能达到最高传输率的传输媒体是哪一种？

**【问题 4】**要获得最佳的数据传输安全保密性的传输媒体是哪一种？

**分析：**局域网的传输媒体主要有双绞线、同轴电缆、光缆和无线传输四大类。最常用的是双绞线和光缆，这与它们各自的特点是分不开的。一般短距离采用双绞线，长距离则使用光缆。

光纤利用全内反射来传输经信号编码的光束，能实现最高速率的传输。所以说目前局域网能达到最高传输率的传输媒体是光缆。

光纤不受电磁干扰或噪声的影响，这种特性允许其在很长的距离内进行高速数据传输，并能提供优良的安全保密性，所以说要想获得最佳的数据传输安全保密性，就要采用光缆作为传输媒体。

答案：

【问题1】传输媒体是收发双方之间进行通信的物理信号通路。用于局域网的传输媒体有双绞线、同轴电缆、光缆和无线传输媒体四类。

【问题2】目前局域网常用的传输媒体为双绞线和光缆。

【问题3】目前局域网上能达到最高传输率的传输媒体是光缆。

【问题4】要想获得最佳的数据传输安全保密性，需使用的传输媒体是光缆。

例4　阅读以下说明，回答问题。

【说明】

某大型企业包括网络中心、管理部、生产部、市场部、财务部、人事部等部门，各部门内部都已经建设了自己的局域网系统。现要将企业内部各部门的局域网互联起来。建设企业内联网。

组网要求：能够实现企业内部各部门局域网系统的有效隔离，防止跨部门的非法访问；各部门之间根据需要可以有效互联通信，将信息由部门级共享提高至企业级共享；各部门的计算机都可以连接访问 Internet。

【问题1】请简述其实施方案并画出网络拓扑结构示意图。

【问题2】简述路由器在局域网组网工程中的应用。

分析：根据用户需求可以总结出用户对现有局域网系统的 3 点要求，即局域网隔离、局域网互联以及局域网与广域网互联。这恰好就是路由器在局域网系统中的 3 项应用。因此可以在组网方案中应用路由器作为网络互联设备。

答案：

【问题1】各部门局域网之间通过路由器互联起来，通过配置路由器实现各部门之间的访问控制策略；路由器具有连接 Internet 的广域网端口，企业内部各部门局域网系统中的计算机可以通过路由器访问 Internet，其拓扑结构如图 1-18 所示。

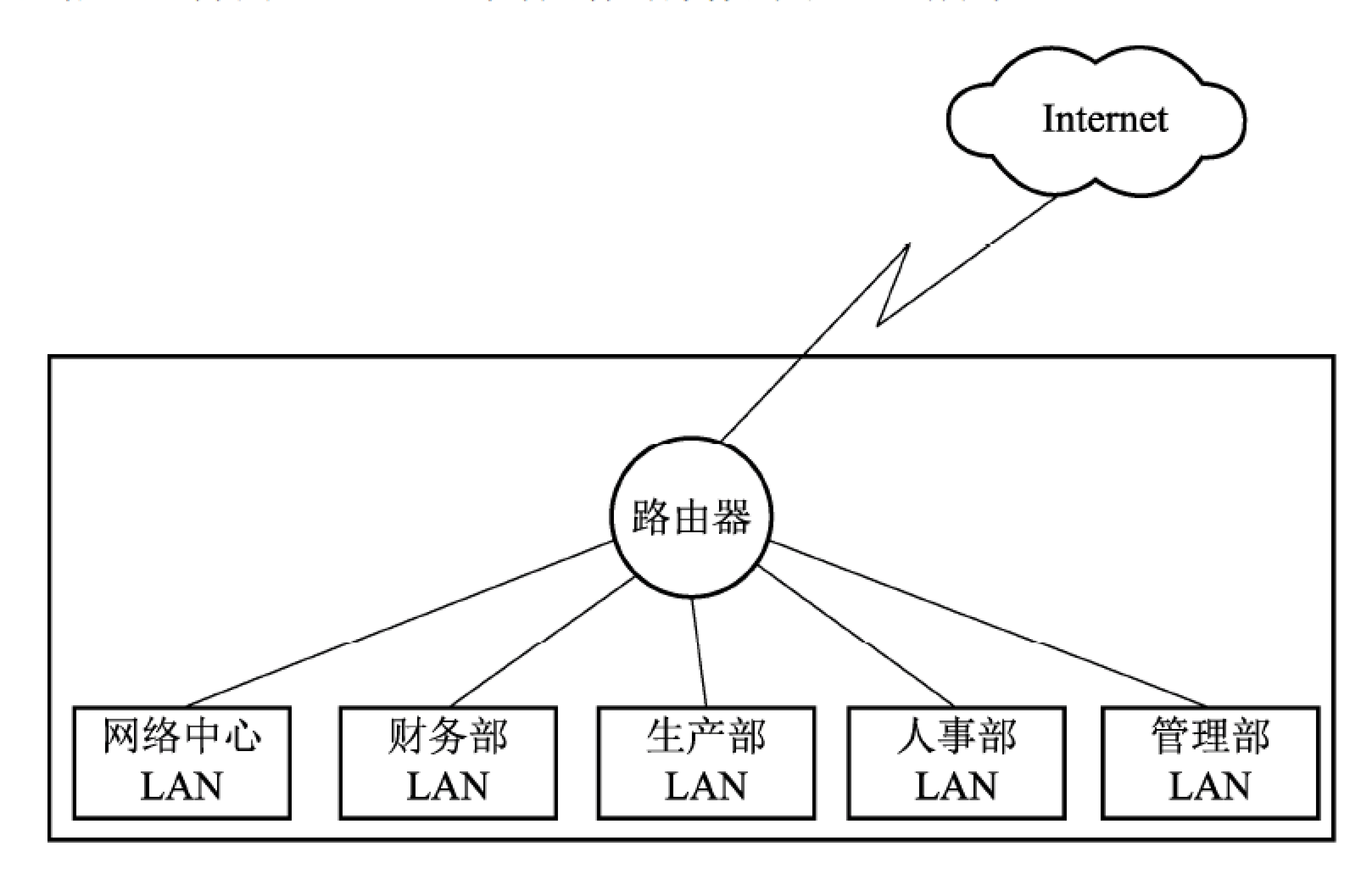



图 1-18　某企业内部网组网拓扑结构

【问题2】路由器在局域网系统中的应用主要如下。

(1) 局域网互联。连接多个局域网系统并实现局域网系统之间的数据转发。互联的局域网系统可以是相同类型，也可以是不同类型。

(2) 局域网隔离。连接多个局域网系统并实现局域网系统之间的数据隔离。

(3) 局域网与广域网互联。局域网通过路由器连接广域网，实现对远程主机的访问。

### 1.2.3　同步练习

1．简要回答下列有关局域网的问题。

**【问题 1】**局域网需要 OSI 参考模型的哪几层？

**【问题 2】**局域网的标准主要是由哪个委员会制定的？

**【问题 3】**列出局域网常用的访问控制方式。

2．简要回答下列有关 10Mb/s 以太网的问题。

**【问题 1】**简述 10Base-T 以太网的组成。

**【问题 2】**简述 10Base-T 以太网系统的特点。

**【问题 3】**在 10Base-T 的收发器中，双绞线起什么作用？

**【问题 4】**试比较 4 种 10Base 以太网的物理性能。

3．按传输媒体类型划分快速以太网类型。

4．交换型以太网的中心设备是什么？与共享型以太网系统比较，交换型以太网系统有何特点？

5．10Mb/s 以太网、快速以太网以及千兆位以太网有何区别与联系？

6．对于工作在半双工模式的 24 口交换机，若每个端口的速率为 10Mb/s，则整个系统带宽可达多少？

7．简要回答下列问题。

**【问题 1】**哪些以太网产品支持全双工操作？

**【问题 2】**简述全双工以太网的技术特点(与传统半双工以太网相比)。

8．已知某局域网采用 CSMA/CD 媒体访问控制技术，其共享媒体最大跨距为 500m，物理层处理延迟时间为 $10^{-5}$s，传输媒体的数据传输率为 10Mb/s，试计算该网络的最小帧长度。

9．简要回答下列问题。

**【问题 1】**收发器的主要功能有哪些？

**【问题 2】**对于 10Mb/s 的以太网，它有哪几种收发器？

**【问题 3】**集线器在以太网系统中具有的主要功能是什么？

### 1.2.4　同步练习参考答案

1．

**【问题 1】**局域网需要 OSI 中的物理层、数据链路层(数据链路层分为媒体访问控制子层和逻辑链路控制子层)。

**【问题 2】**IEEE 802 委员会。

【问题3】局域网常用的访问控制方式有 3 种，分别是载波帧听访问/冲突检测(CSMA/CD)、令牌环访问控制法(Token Ring)和令牌总线访问控制法(Token Bus)。

2.

【问题1】10Base-T 以太网的组成如下。

(1) 10Base-T 以太网系统由集线器、网卡和非屏蔽双绞线(3 类以上)组成。

(2) 网卡与集线器、集线器与集线器之间通过 RJ-45 连接器和双绞线实现互联和通信。

(3) 10Base-T 以太网系统中，单段媒体最大长度为 100m，可以通过 4 个集线器级联，连接 5 个媒体可使最大跨距达 500m。

【问题2】10Base-T 以太网系统的特点如下。

(1) 采用星型或树型拓扑结构，核心为集线器。

(2) 传输媒体采用 3 类、4 类或 5 类非屏蔽双绞线，发送与接收通道物理上分开，各占一根双绞线。

(3) 网络站点通过网卡上的 RJ-45 连接器和双绞线直接连接集线器。

【问题3】双绞线的作用如下。

(1) 网卡上发送和接收分别使用一根双绞线，即一根双绞线发送信号，另一根作为信号接收使用。

(2) 当网卡与集线器相连接时，网卡上作为发送的那根双绞线正作为集线器接收使用；反之，网卡上作为接收的那根双绞线正作为集线器发送使用。

【问题4】10Base 以太网的物理性能如下。

(1) 10Base-5 使用外置收发器，传输媒体为价格较贵、需要专业化安装的直径 10mm、阻抗 50Ω的粗同轴电缆，采用总线型拓扑结构，单段媒体最大长度为 500m，最多可使用 4 个中继器连接 5 段媒体，使跨距最大达 2.5km，网卡通过 AUI 接口与媒体连接。

(2) 10Base-2 在网卡上内置收发器，传输媒体使用价格便宜、安装简单的直径 5mm、阻抗 50Ω的细同轴电缆，采用总线型拓扑结构，单段媒体最大长度为 185m，最多可使用 4 个中继器连接 5 段媒体，使跨距最大达 925m，网卡通过 BNC 连接器和 T 形头与媒体连接。

(3) 10Base-T 在网卡上内置收发器，传输媒体使用便宜、安装简单的非屏蔽双绞线(3 类以上 UTP)，采用星型拓扑结构，单段媒体最大长度为 100m，可以通过 4 个集线器级联，连接 5 个媒体，使最大跨距达 500m，网卡通过 RJ-45 连接器与媒体连接。

(4) 10Base-F 在网卡上内置收发器，传输媒体使用 62.5/125 多模光纤，采用星型拓扑结构，单段媒体最大长度为 2km，可以通过一个集线器级联，连接两个媒体段，使最大跨距达 4km，网卡通过 ST 连接器与光纤连接。

3.

按传输媒体类型划分，快速以太网可分为 100Base-TX、100Base-FX、100Base-T4 这 3 种类型。

(1) 100Base-TX 采用 5 类非屏蔽双绞线，使用两对线对。

(2) 100Base-FX 采用多模光纤或单模光纤。

(3) 100Base-T4 采用 3 类非屏蔽双绞线，使用全部 4 对线对。

4．交换型以太网的中心设备是以太网交换机。交换型以太网系统与共享型以太网比较

有以下优点。

(1) 每个端口上可以连接站点，也可以连接一个网段。不论站点和网段是否独占该端口的带宽。

(2) 系统的最大带宽可以达到端口带宽的 $n$ 倍，其中 $n$ 为端口数。$n$ 越大，系统的带宽越高。

(3) 交换机连接了多个网段，每一个网段都是独立的、被隔离的。但如果需要的话，独立网段之间通过其端口也可以建立暂时的数据通道。

(4) 被交换机隔离的独立网段上数据流信息不会随意广播到其他端口上去，因此具有一定的数据安全性。

5．

(1) 快速以太网和千兆位以太网属于高速以太网，是在 10Mb/s 以太网基础上发展起来的数据传输率更高的以太网技术。

(2) 快速以太网是在 10Base-T 和 10Base-F 技术基础上发展起来的具有 100Mb/s 数据传输率的以太网，快速以太网的传输媒体和媒体布局向下兼容 10Mb/s 以太网，帧结构和媒体访问控制方式则完全遵循 IEEE 802.3 基本标准。

(3) 千兆位以太网是快速以太网的自然发展，只是数据传输率达到 1000Mb/s，二者的拓扑结构完全一致，传输媒体的媒体布局在快速以太网基础上有所发展，但向下兼容快速以太网和 10Mb/s 以太网，帧结构和媒体访问控制方式也与 IEEE 802.3 基本类同，但有所发展。

6．240Mb/s(24×10Mb/s)

7．

**【问题 1】**

(1) 只有链路上提供独立的发送和接收媒体的以太网产品才能支持全双工操作。

(2) 在 10Mb/s 以太网中只有 10Base-T 和 10Base-F 支持全双工操作。

(3) 在 100Mb/s 以太网中 100Base-TX、100Base-FX 都支持全双工操作。

(4) 在 1000Mb/s 以太网中 1000Base-LX、1000Base-SX、1000Base-CX、1000Base-TX 都支持全双工操作。

**【问题 2】**全双工以太网技术是用来说明以太网设备端口的传输技术，与传统半双工以太网技术区别在于：每个端口和交换机背板之间都存在两条逻辑通路。这样每个端口就可以同时接收和发送帧，不再受 CSMA/CD 的约束，在端口发送帧时不会再发生帧的碰撞，已无碰撞域存在。这样端口之间媒体的长度仅仅受数字信号在媒体上传输衰变的影响，而不像传统以太网半双工传输时还要受碰撞域的约束。

8．根据最小帧长度的计算公式：

$$L_{min}=\text{slot time}\times R\approx(2S/0.7C+2t_{PHY})\times R$$

$$=[2\times500/(0.7\times3\times10^8)+2\times10^{-5}]\times10\times10^6$$

$$=248(\text{位})$$

所以该网络最小帧长度为 248 位。

9.

【问题 1】收发器的主要功能有：向媒体发送信号、自媒体接收信号、识别媒体是否存在信号。

【问题 2】对于 10Mb/s 的以太网有 10Base-5、10Base-2、10Base-T、10Base-F 几种收发器。

【问题 3】集线器在以太网系统中具有的主要功能有：一是媒体上信号的再生和再定时；二是检测碰撞；三是端口的扩展功能；四是混合连接 10Base-5 与 10Base-2 以太网系统。

# 1.3　以太网交换机的部署

## 1.3.1　考点辅导

### 1.3.1.1　交换机的连接模式

交换机的连接模式有级联模式、堆叠模式和混合模式。

1. 级联模式

级联模式是最常规、最直接的一种扩展方式。级联模式是通过双绞线或光纤来级联，一般在交换机的前面板上有专门的级联口，如果没有也可以用交叉线接法来级联。级联是通过端口进行的，级联后两台交换机是上下级的关系。

级联模式起源于早期的共享型集线器，其物理拓扑结构是星型的，而逻辑拓扑结构是总线型的。集线器仅相当于一条浓缩的总线，在集线器的某一个端口级联另一台集线器，只是相当于把浓缩的总线又加长了一些，但其仍然是一条总线，所有端口都要在一个碰撞域里受 CSMA/CD 的约束。但这样相当于把传输媒体加长了，在加长的传输媒体上又增加了一些端口。但付出的代价是，在这个碰撞域里又多了一些端口共享整个带宽，从而导致网络性能低下。当然，这种级联方式必须遵循 5-4-3 法则，也就是级联不能超过 4 层。

在交换机上进行级联，级联交换机的端口共享的仅仅是被级联交换机端口的带宽，而不是整个网络的带宽。更何况目前的交换机级联通常是高速交换机级联低速交换机，即 1000Mb/s 端口级联 100/1000Mb/s 的交换机；100Mb/s 端口级联 10/100Mb/s 的交换机；或者是交换机级联共享型的集线器。由此级联模式极大程度地克服了传统集线器级联共享带宽而导致网络性能降低的弊端。

2. 堆叠模式

堆叠通常是为了扩充带宽用的，通常用专门的堆叠卡插在交换机的后面，用专门的堆叠电缆连接几台交换机，堆叠后这几台交换机相当于一台交换机。堆叠是采用交换机背板的叠加，使多个工作组交换机形成一个工作组堆，从而提供高密度的交换机端口。堆叠中的交换机就像一个交换机一样，配置一个 IP 地址即可。

级联是通过交换机的某个端口与其他交换机相连的，而堆叠是通过集线器的背板连接

起来的，它是一种建立在芯片级上的连接。如两个 24 口交换机堆叠起来的效果就像是一个 48 口的交换机。

常见的堆叠有两种，即菊花链堆叠和矩阵堆叠。

3. 混合模式

在实际应用中，由于网络的复杂性、用户需求的多重性，通常同时使用两种模式进行交换机的部署，故称其为混合模式。

#### 1.3.1.2　以太网交换机的设置

对一台新的交换机进行配置和管理有两个主要步骤：一是通过仿真终端进行 IP 地址设置；二是通过浏览器进行管理。

1. 通过仿真终端进行 IP 地址设置

通过仿真软件设置 3COM 交换机 IP 地址的步骤如下。

(1) 用一条 RS-232 型电缆将管理终端的串口与交换机的控制台端口(Console)相连。

(2) 运行仿真终端软件，通常使用“附件”中的“超级终端”命令即可。

(3) 选择所连接的串口，如 COM1 端口。

(4) 根据说明书设置仿真终端的位率、数据位、奇偶校验和停止位等参数。

(5) 设置远程登录的用户名、密码及其他常见用户名。

(6) 设置 IP 地址及子网掩码。

2. 通过浏览器进行管理

(1) 打开浏览器，在 URL 栏中输入交换机 IP 地址后按 Enter 键，出现交换机的 Web 登录界面，在其中输入相应的用户名和密码后单击“确定”按钮。

(2) 进入交换机的 Web 管理页面。

(3) 在 Web 管理页面中，既可以查看交换机的基本信息，也可以进行一些参数设置，如修改交换机管理用户的口令。

### 1.3.2　典型例题分析

**例 1**　以太网交换机一定要设置才能工作，这一叙述是否正确？

**分析：**一台新的交换机部署到网络中后，使用默认配置就可以工作，不需要再进行设置。因为它是一种将软件装在 Flash Memory(闪存)中的硬件设备，当加电时，首先进行一系列自检，对所有的端口进行测试之后，交换机就处于工作状态。这时设备的交换表是空的，它可以通过自学来了解各个端口的设备连接情况，并将设备的 MAC 地址记录在交换表中，当有信息交换时交换机就根据交换表来进行数据转发。

但是，当有一些高级应用和需求时，如通过交换机划分 VLAN 或是对交换机进行远程管理等，就需要对交换机进行设置。

**答案：**错误，以太网交换机在一般应用时不需进行任何设置即可使用。

**例 2** 交换机之间级联只能采用双绞线，这一叙述是否正确？采用什么类型的级联双绞线？

**分析：**交换机之间级联可通过双绞线或光纤。用双绞线进行级联时可根据实际情况采用直通线或交叉线。

**答案：**错误。级联双绞线可根据需要采用直通线或交叉线。

**例 3** 非屏蔽双绞线的直通线和交叉线可用于下列哪两种设备间的通信？集线器到集线器(不使用级联端口)使用__(1)__；PC 到集线器使用__(2)__；PC 到交换机使用__(3)__；PC 到 PC 使用__(4)__。

**分析：**对于那些没有专用级联端口的集线器之间的级联，双绞线接头中线对的分布与连接网卡和集线器有所不同，必须要用交叉线。而许多集线器为了方便用户，提供了一个专门用来连接到另一台集线器的普通端口，对此类集线器进行级联时双绞线均采用直通线。

**答案：**(1)交叉线　(2)直通线　(3)直通线　(4)交叉线

**例 4** 交换机与 Hub 如何进行级联才能达到最佳效果？

**分析：**在 Hub 和交换机性能优化方面主要体现在 Hub 或交换机的级联上。如果需要 Hub 与 Hub 或 Hub 与交换机级联，则一定要注意 Hub 的带宽是所有端口共用的，因此每个端口实际利用的带宽均是应用总带宽(如 100Mb/s)除以所用端口数。所以一般不用 Hub 来级联，而是通过用 Hub 连接在交换机的端口上，因为交换机所指的带宽就是每个端口的实际可用带宽，如 $n$10Mb/s+$m$100Mb/s 就表明在这个交换机上有 $n$ 个 10Mb/s 的带宽，有 $m$ 个 100Mb/s 的带宽端口，这些带宽是具体端口独享的，而不受交换机所用端口数的限制。

也就是说，如果一个 Hub 连在一个交换机的 100Mb/s 端口上，则这个 Hub 上就拥有总共 100Mb/s 的带宽；如果一个 Hub 连接在有 100Mb/s 带宽的 Hub 端口上，则连接一个 Hub 可能使用了 10 个端口，实际上下一个 Hub 的总带宽就远达不到 100Mb/s 的带宽，这样就影响了连接在下一个 Hub 上的工作站速度。所以 Hub 级联一般最多为两层，层数多了会使速度呈倍差级数减慢。

另外还有两点要注意：一是当 Hub 要通过交换机级联时最好连接在 100Mb/s 带宽的端口，除非没有 100Mb/s 端口可用；二是要注意双绞线最大单段网线长度在 100m 以内，否则信号会衰减严重，影响网络速度。

**答案：**一个 Hub 连在一个交换机的 100Mb/s 或 10Mb/s 端口上，同时相互级联的网线长度在 100m 之内。

## 1.3.3　同步练习

1．什么是级联？
2．简述级联的优势。
3．常见的堆叠有哪两种？堆叠技术的最大优点是什么？

4．简述堆叠模式的优、缺点。

5．在网络中利用以太网交换机进行部署时常采用哪 3 种模式？

6．对没有任何设置的交换机通过何种方式进行配置？

7．设置了 IP 地址以后的交换机可采用哪两种方式进行远程管理？

8．描述通过仿真软件设置 3COM 交换机 IP 地址的步骤。

9．通过 Web 页面可对设置 IP 地址的 3COM 3300 交换机进行远程管理，请列举出通过远程管理可实现哪些功能。

## 1.3.4　同步练习参考答案

1．级联是通过双绞线或光纤把需要级联的设备通过端口相连接，从而达到增加同一网络端口数目的方法。

2．级联的优势如下。

(1) 级联模式可使用通用的以太网端口进行层次间互联，其中包括 100Mb/s 端口、1000Mb/s 端口以及新兴的 10Gb/s 端口。

(2) 级联模式是组建结构化网络的必然选择，级联使用普通的、长度限制并不严格的电缆(光纤)，各个级联单元的位置相对较随意，非常有利于综合布线。

(3) 级联模式通常是解决不同品牌的交换机之间以及交换机与集线器之间连接的有效手段。

3．常见的堆叠有两种，即菊花链堆叠和矩阵堆叠。堆叠技术的最大优点就是提供简化的本地管理，将一组交换机作为一个对象来管理。

4．

堆叠模式的优点如下。

(1) 增加网络端口的同时，还增加了逻辑通道，扩充了网络带宽，不同堆叠单元的端口之间可以直接交换，进行快速转发，从而极大地提高了网络性能。

(2) 不受 5-4-3 法则的约束，堆叠单元可以超过 4 个。

(3) 提供简化的本地管理，将一组交换机作为一个对象来管理。

堆叠模式的缺点如下。

(1) 堆叠是一种非标准化技术，各个厂商之间不支持混合堆叠，同一组堆叠交换机必须是同一品牌。

(2) 堆叠模式不支持即插即用，在物理连接完毕之后还要对交换机进行相应的设置才能正常运行。

(3) 不存在拓扑管理，一般不能进行分布式布置。

5．常采用 3 种模式，即级联模式、堆叠模式和混合模式。

6．对没有任何设置的交换机通过仿真终端可设置交换机的登录用户名、密码、IP 地址及子网掩码等。

7．交换机可通过 Telnet 命令行的方式及 Web 页面的方式进行远程管理。

8．设置步骤如下。

(1) 用一条 RS-232 型电缆将管理终端的串口与交换机的控制台端口(Console)相连。

(2) 运行仿真终端软件，如超级终端。

(3) 选择所连接的串口。

(4) 根据说明书设置仿真终端的位率、数据位、奇偶校验位和停止位等参数。

(5) 设置远程登录的用户名、密码及其他常见用户名。

(6) 设置 IP 地址及子网掩码。

9．远程管理可实现以下功能。

(1) 可查看连入交换机机器网卡的 MAC 地址。

(2) 可查看每一个端口的状态。

(3) 可根据需要关闭、打开端口。

(4) 可以修改交换机管理用户的口令。

(5) 可根据需要对端口进行 VLAN 的划分等。

# 1.4 交换机与路由器的基本配置

## 1.4.1 考点辅导

### 1.4.1.1 交换机的基本配置

本节主要以华为 S 系列交换机为例介绍交换机配置的基本技术和技能。

1. 电缆连接及终端配置

如图 1-19 所示，接好 PC 机和交换机各自的电源线，在关机状态下，把 PC 机的串口 1(COM1)通过控制台电缆与交换机的 Console 端口相连，即完成设备的连接工作。




图 1-19 仿真终端与交换机的连接

交换机 Console 端口的默认参数如下。

- 端口速率：9600bps。
- 数据位：8。
- 奇偶校验码：无。
- 停止位：1。
- 流控：无。

在配置 PC 机的超级终端时只需保证端口属性的配置参数与上述参数相同匹配即可。以 Windows 环境下的 Hyper Terminal 为例配置 COM1 端口属性的对话框，如图 1-20 所示。



图 1-20　COM1 属性

2. 交换机的启动

在配置好终端仿真软件后，终端窗口就会显示交换机的启动信息，显示交换机的版权信息和软件加载过程，直到出现提示用户设置登录密码。

```
BIOS loading ……
……
Enter Password:
Confirm Password:
<HUAWEI>
```

完成 Console 登录密码设置后，用户便可以配置和使用交换机。

3. 交换机的基本配置

在默认配置下，所有接口处于可用状态，并且都属于 VLAN1，这种情况下交换机就可以正常工作了。但为了方便管理和使用，首先应对交换机做基本的配置。

(1) 配置交换机的设备名称、管理 VLAN 和 TELNET，在对网络中交换机进行管理时需要对交换机进行基本配置。

```
<HUAWEI>
<HUAWEI> system-view
[HUAWEI] vlan 5    //创建交换机管理 VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5
[HUAWEI-vlanif5] ip address 10.10.1.1 24
[HUAWEI-vlanif5] quit
[HUAWEI] telnet server enable   //Telnet 出厂时是关闭的，需要打开
[HUAWEI] user-interface vty 0 4   //Telnet 常用于设备管理员登录，推荐使用 AAA 认证
[HUAWEI-ui-vty0-4] protocol inbound telnet    //V2R6 及之前版本缺省支持 telnet
协议，但是 V2R7 及之后版本缺省的是 SSH 协议，因此使用 telnet 登录之前，必须要先配置这条
命令
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
```

```
[HUAWEI-aaa] local-user admin password irreversible-cipher Helloworld@6789
//配置管理员 Telnet 登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin privilege level 15    //将管理员的账号权限设置为
15(最高)
[HUAWEI-aaa]local-user admin service-type telnet
[HUAWEI-aaa]quit
[HUAWEI]quit
<HUAWEI>save
```

(2) 登录 Telent 到交换机，出现用户视图提示符。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1
//输入交换机管理 IP，并回车
Login authentication
Username:admin    //输入用户名和密码
Password:
Info: The max number of VTY users is 5, and the number
of current VTY users on line is 1.
The current login time is 2014-05-06 18:33:18+00:00.
<HUAWEI>
```

(3) 配置交换机的接口。交换机的接口属性默认支持一般网络环境，一般情况下是不需要对其接口进行设置的。在某些情况下需要对其端口属性进行配置时，配置的对象主要有接口隔离、速率、双工等信息。

```
#配置接口 GE1/0/1 和 GE1/0/2 的端口隔离功能，实现两个接口之间的二层数据隔离，三层数据互通
<Switch1>system-view
[Switch1]port-isolate mode 12
[Switch1]interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1]port-isolate enable group 1
[Switch-GigabitEthernet1/0/1]quit
[Switch1]interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2]port-isolate enable group 1
[Switch-GigabitEthernet1/0/2]quit

#配置以太网接口 GE0/0/1 在自协商模式下协商速率为 100Mb/s
<Switch1>system-view
[Switch1] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1]negotiation auto
[Switch-GigabitEthernet1/0/1]auto speed 100

#配置以太网接口 GE0/0/1 在自协商模式下双工模式为全双工模式
<Switch1>system-view
[Switch1] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1]negotiation auto
```

(4) 查看和配置 MAC 地址表。交换机通过学习网络中设备的 MAC 地址，并将学习得到的 MAC 地址存放在交换机的缓存中。在需要向目标地址发送数据时就从 MAC 表地址中查找相应的地址，找到后才可以向目标快速发送数据。

MAC 表由多条 MAC 地址表项组成。MAC 地址表项由 MAC、VLAN 和端口组成，交换机在收到数据帧时，会解析出数据帧的源 MAC 地址和 VLAN ID 并与接收数据帧的端口组合成一条数据表项。MAC 地址表项的查看可以了解交换机运行的状态信息，排查故障。

```
#执行命令 display mac-address，查看所有的 MAC 地址表项
<Switch1>display mac-address
-------------------------------------------------------------------------
MAC Address      VLAN/VSI            Learned-From            Type
-------------------------------------------------------------------------
00e0-0900-7890   10/-                -                      black
00e0-0230-1234   20/-                GE1/0/1                 static
0001-0002-0003   30/-                Eth-Trunk1              dynamic
-------------------------------------------------------------------------
Total items displayed = 3

#执行命令 display interface vlanif5，显示 VLANIF 接口的 MAC 地址
<Switch1>display interface vlanif5
Vlanif5 current state:DOWN
Line protocol current state:DOWN
Description:
Route Port,Address is 192.168.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2,Hardware address is 00e0-0987-7891
Current system time:2016-07-03 13:33:09+08:00
        Input bandwidth utilization :--
        Output bandwidth utilization :--

#在 MAC 地址表中增加静态 MAC 地址表项，目的 MAC 地址为 0001-0002-0003，VLAN 5 的报文，
从接口 gigabitethernet0/0/5 转发出去
[Switch1]mac-address static 0001-0002-0003 gigabitethernet 0/0/5 vlan 5
```

#### 1.4.1.2　配置和管理 VLAN

VLAN 技术上是交换技术的重要组成部分，也是交换机配置的基础。它用于把物理上直接相连的网络从逻辑上划分为多个子网。每一个 VLAN 对应着一个广播域，处于不同 VLAN 上的主机不能进行通信，不同 VLAN 之间的通信要引入第三层交换技术才可以解决。对虚拟局域网的配置和管理主要涉及链路和接口类型、GARP 协议和 VLAN 的配置。

链路和接口类型，为了适应不同网络环境的组网需要，链路类型分为接入链路(Access Link)和干道链路(Trunk Link)两种链路类型。接入链路只能承载一个 VLAN 的数据帧，用于连接交换机和用户终端；干道链路能承载多个不同 VLAN 的数据帧，用于交换机间互连或连接交换机与路由器。根据接口连接对象以及对收发数据帧处理的不同，以太网接口分为 Access 接口、Trunk 接口、Hybrid 接口和 QinQ 接口 4 种接口类型，分别用于连接终端用户、交换机与路由器以及公网与私网的互联等。

GARP 协议主要用于建立一种属性传递扩散机制，以保证协议实体能够注册和注销该属性。简单说就是为了简化网络中配置 VLAN 的操作，通过 GVRP 的 VLAN 自动注册功能将设备上的 VLAN 信息快速复制到整个交换网，达到减少手工配置及保证 VLAN 配置正确的

目的。

交换机的初始状态是工作在透明模式，有一个默认的VLAN1，所有端口都属于VLAN1。

1. 划分 VLAN 的方法

虚拟局域网是交换机的重要功能，通常虚拟局域网的实现形式有多种，分别是基于接口、MAC 地址、子网、网络层协议、匹配策略方式来划分 VLAN。

通过接口来划分 VLAN。交换机的每个接口配置不同的 PVID，当数据帧进入交换机时没有带 VLAN 标签，该数据帧就会被打上接口指定 PVID 的 Tag 并在指定 PVID 中传输。

通过源 MAC 地址来划分 VLAN。建立 MAC 地址和 VLAN ID 映射关系表，当交换机收到的是 Untagged 帧时，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过子网划分VLAN。建立IP地址和VLAN ID映射关系表，当交换机收到的是Untagged帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过网络层协议划分 VLAN。建立以太网帧中的协议域和 VLAN ID 的映射关系表，当收到的是 Untagged 帧，就依据该表给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

通过策略匹配划分 VLAN，实现多种组合的划分，包括接口、MAC 地址、IP 地址等。建立配置策略，当收到的是 Untagged 帧，且匹配配置的策略时，给数据帧添加指定 VLAN 的 Tag 并在指定 VLAN 中传输。

2. 配置 VLAN 举例

在网络中，用于终端与交换机、交换机与交换机、交换机与路由器连接时 VLAN 的划分方式多种多样，需要灵活运用。这里就接入层交换机的 VLAN 划分举例说明。

(1) 以接入交换机 ACC1 为例，创建 ACC1 的业务 VLAN10 和 20。

```
<HUAWEI> system-view
[HUAWEI] sysnameACC1//修改设备名称为 ACC1
[ACC1] vlan batch 10 20//批量创建 VLAN
```

(2) 配置 ACC1 连接 CORE1 和 CORE2 的 GE0/0/3 和 GE0/0/4，透传部门 A 和部门 B 的 VLAN。

```
[ACC1] interface GigabitEthernet 0/0/3
[ACC1-GigabitEthernet0/0/3] port link-type trunk
//配置为 trunk 模式，用于透传 VLAN
[ACC1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
//配置 GE0/0/3 透传 ACC1 上的业务 VLAN
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface GigabitEthernet 0/0/4
[ACC1-GigabitEthernet0/0/4] port link-type trunk
//配置为 trunk 模式，用于透传 VLAN
[ACC1-GigabitEthernet0/0/4] port trunk allow-pass vlan 10 20
//配置 GE0/0/4 透传 ACC1 上的业务 VLAN
[ACC1-GigabitEthernet0/0/4] quit
```

(3) 配置 ACC1 连接用户的接口，使各部门加入 VLAN。

```
[ACC1] interfaceGigabitEthernet0/0/1    //配置连接部门 A 的接口
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 10
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interfaceGigabitEthernet0/0/2    //配置连接部门 B 的接口
[ACC1-GigabitEthernet0/0/2] port link-type access
[ACC1-GigabitEthernet0/0/2] port default vlan 20
[ACC1-GigabitEthernet0/0/2] quit
```

(4) 配置 BPDU 保护功能，加强网络的稳定性。

```
[ACC1] stpbpdu-protection
```

如果把 ACC1 下接入的用户都加入 VLAN 10，为了配置简单，也可以 ACC1 上不配置 VLAN，而把 CORE1、CORE2 与 ACC1 直接相连的接口以 access 方式加入 VLAN10，这样通过 ACC1 接入的用户全部属于 VLAN10。

#### 1.4.1.3　路由器概述

路由器是工作在 OSI 模型中的第三层(网络层)的设备，它具有局域网和广域网两种接口。可以作为企业内部网络和 Internet 骨干网络的连接设备来使用。路由器通过路由表为进入路由器的数据分组选择最佳的路径并将分组传输到适当的出口。

1. 路由器的功能

路由器主要有三种功能：网络互联、网络隔离和流量控制。

(1) 网络互联：主要采用地址映射和路由选择来实现不同网络之间的数据包传输。

(2) 网络隔离：路由器可以根据数据包的源地址、目的地址、数据包类型等对数据包能否被转发做出适当的判断，从而隔离各个局域网之间不需要传输的数据包。

(3) 流量控制：利用路由算法来均衡网络负载，从而有效地控制网络拥塞。

2. 路由器表

路由表中保存着子网的标志信息、网络中路由器的个数和下一个路由器的名字等内容。路由表可以是由系统管理员固定设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。

1) 静态路由表

由系统管理员事先设置好固定的路由表称为静态(Static)路由表这种路由表。一般是在系统安装时就根据网络的配置情况预先设定的，它不会随网络结构的改变而改变。

2) 动态路由表

动态(Dynamic)路由表是路由器根据网络系统的运行情况而自动生成的路由表。路由器根据路由选择协议(Routing Protocol)提供的功能，自动学习和记忆网络的运行情况，在需要时自动计算数据传输的最佳路径。

3. 路由选择协议

路由选择协议是一种网络层协议，它通过提供一种共享路由选择信息的机制，允许路

由器与其他路由器通信以更新和维护自己的路由表，并确定最佳的路由选择路径。路由协议根据其生成路由表的方式，可以分为静态路由协议和动态路由协议两种。

1) 静态路由协议

在静态路由协议下，路由信息由管理员配置而成，它适用于小型的局域网络(拥有 5 台以下的路由器)。静态路由协议具有运行速度快、占用资源少、配置方法简单的特点，但在较大规模的网络中并不能够很好地运行和维护。

2) 动态路由协议

动态路由协议根据路由信息更新方式的不同，可以分为距离矢量路由协议和链路状态路由协议两种。

(1) 距离矢量路由协议：距离矢量(Distance-vector)路由协议采用距离矢量路由选择算法，它确定到网络中任一链路的方向(向量)与距离，如 RIP 协议。

(2) 链路状态路由协议：链路状态(Link-state)路由协议创建整个网络的准确拓扑，以计算路由器到其他路由器的最短路径，如 OSPF、IS-IS 等。

#### 1.4.1.4 路由器的配置

1. 路由器的基本配置

与交换机的配置类似，路由器的配置操作有 3 种模式，即用户视图、系统视图和具体业务视图。用户视图模式下，在用户视图下，用户可以完成查看运行状态和统计信息等功能，这些命令对路由器的正常工作没有影响；在系统视图模式下，用户可以配置系统参数以及通过该视图进入其他的功能配置视图；在具体业务视图模式下，用户可以配置接口相关的物理属性、链接层特性及 IP 地址等重要参数，路由协议的大部分参数也需要在这种模式下配置。

其中，配置模式又分为全局配置模式和接口配置模式、路由协议配置模式、线路配置模式等子模式。在不同的工作模式下，路由器有不同的命令提示状态。

<Switch>。在交换机正常启动后，用户使用终端仿真软件或 Telent 登录交换机，可自动进入用户配置模式，这时用户可以看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器的设置内容。

[Switch]。路由器处于系统视图命令状态，在<Switch>提示符下输入 system-view，可进入系统视图状态，这时不仅可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

[Switch-vlan]。路由器处于具体的业务视图状态，在[Swith]提示符下输入需要配置的业务命令，可进入该状态。退出具体的业务输入 quit。

在开机自检时，按 Ctrl+Break 组合键可进入 BootROM menu 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导，或者进行路由器口令恢复时要进入该状态。

2. 静态路由的配置

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径，网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

1) IPv4 静态路由设置

在创建静态路由时，可以同时指定出接口和下一跳。对于不同的出接口类型，也可以

只指定出接口或只指定下一跳。

- 对于点到点接口，指定出接口。
- 对于 NBMA(Non Broadcast Multiple Access)接口，指定下一跳。
- 对于广播接口(如以太网接口)，指定下一跳。

在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv4 静态缺省路由。缺省情况下，没有创建 IPv4 静态缺省路由。

操作步骤如下。

(1) 执行命令 system-view，进入系统视图。

(2) 配置 IPv4 静态路由。

- 在公网上配置 IPv4 静态路由：ip route-static ip-address { mask | mask-length } { nexthop-address | interface-type interface-number [ nexthop-address ] | vpn-instance vpn-instance-name nexthop-address } [ preference preference | tag tag ] * [ description text ]
- 在 VPN 实例中配置 IPv4 静态路由：ip route-static vpn-instance vpn-source-name destination-address { mask | mask-length } { nexthop-address [ public ] | interface-type interface-number [ nexthop-address ] | vpn-instance vpn-instance-name nexthop-address } [ preference preference | tag tag ] * [ description text ]

2) IPv6 静态路由设置

在创建静态路由时，可以同时指定出接口和下一跳。对于不同的出接口类型，也可以只指定出接口或只指定下一跳。

- 对于点到点接口，指定出接口。
- 对于 NBMA(Non Broadcast Multiple Access)接口，指定下一跳。
- 对于广播类型接口，指定出接口。如果也指定下一跳，下一跳地址可以不是链路本地地址。

在创建相同目的地址的多条静态路由时，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv6 静态缺省路由。缺省情况下，没有创建 IPv6 静态缺省路由。

操作步骤如下。

(1) 执行命令 system-view，进入系统视图。

(2) 配置 IPv6 静态路由。

- 在公网上配置 IPv6 静态路由：ipv6 route-static dest-ipv6-address prefix-length { interface-type interface-number [ nexthop-ipv6-address ] | nexthop-ipv6-address } [ preference preference | tag tag ] * [ description text ]
- 在 VPN 实例中配置 IPv6 静态路由：ipv6 route-static vpn-instance vpn-instance-name dest-ipv6-address prefix-length { [ interface-type interface-number ] nexthop-ipv6-address | nexthop-ipv6-address [ public ] | vpn-instance

vpn-destination-name nexthop-ipv6-address } [ preference preference | tag tag ] *
[ description text ]

#### 1.4.1.5 配置路由协议

1. 配置 RIP 协议

RIP 是距离矢量路由选择协议的一种。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时，路由器也把所收集的路由信息用 RIP 协议通知相邻的其他：路由器。这样，正确的路由信息逐渐扩散到了全网。

RIP 使用非常广泛，它简单、可靠，便于配置。RIP 版本 2 还支持无类别域间路由(ClasslessInter-Domain Routing, CIDR)、可变长子网掩码(Variable Length Subnetwork Mask, VLSM)和不连续的子网，并且使用组播地址发送路由信息。但是 RIP 只适用于小型的同构网络，因为允许的最大跳数为 15，任何超过 15 个站点的目的地均被标记为不可达。RIP 每隔 30s 广播一次路由信息。

RIP 应用于 OSI 网络七层模型的应用层。各厂家定义的管理距离(AD，即优先级)略有不同，华为定义的优先级是 100。

假设有如图 1-21 所示的网络拓扑结构，试通过配置使 RouterA、RouterB、RouterC 和 RouterD 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。

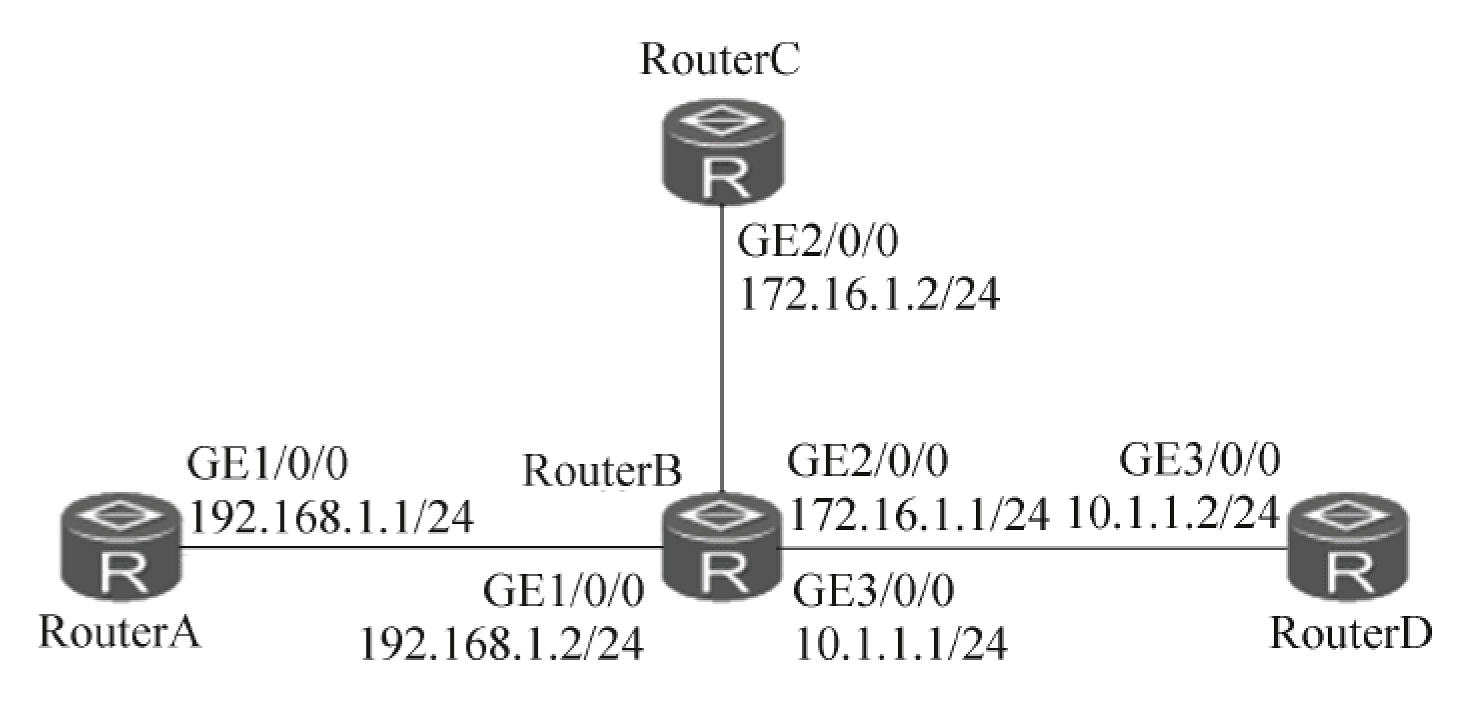



图 1-21 网络拓扑结构

1) 配置思路

采用如下的思路配置 RIP 的版本：

(1) 配置各接口的 IP 地址，使网络可达。

(2) 在各路由器上使能 RIP，配置 RIP 基本功能。

(3) 在各路由器上配置 RIP-2 版本，查看精确的子网掩码信息。

2) 数据准备

为完成此配置例，需准备如下的数据：

(1) 在 RouterA 上指定使能 RIP 的网段 192.168.1.0。

(2) 在 RouterB 上指定使能 RIP 的网段 192.168.1.0，172.16.0.0，10.0.0.0。

(3) 在 RouterC 上指定使能 RIP 的网段 172.16.0.0。

(4) 在 RouterD 上指定使能 RIP 的网段 10.0.0.0。

(5)　在 RouterA、RouterB、RouterC 和 RouterD 上配置 RIP-2 版本。

3)　操作步骤

(1)　配置各接口的 IP 地址(略)。

(2)　配置 RIP 基本功能。

```
# 配置 RouterA。
    [RouterA] rip
    [RouterA-rip-1] network 192.168.1.0
    [RouterA-rip-1] quit
# 配置 RouterB。
    [RouterB] rip
    [RouterB-rip-1] network 192.168.1.0
    [RouterB-rip-1] network 172.16.0.0
    [RouterB-rip-1] network 10.0.0.0
    [RouterB-rip-1] quit
# 配置 RouterC。
    [RouterC] rip
    [RouterC-rip-1] network 172.16.0.0
    [RouterC-rip-1] quit
# 配置 RouterD。
    [RouterD] rip
    [RouterD-rip-1] network 10.0.0.0
    [RouterD-rip-1] quit
# 查看 RouterA 的 RIP 路由表。
    [RouterA] display rip 1 route
    Route Flags: R - RIP
            A - Aging, S - Suppressed, G - Garbage-collect
-----------------------------------------------------------------------
 Peer 192.168.1.2  on GigabitEthernet1/0/0
     Destination/Mask       Nexthop      Cost   Tag     Flags    Sec
       10.0.0.0/8         192.168.1.2      1     0        RA      14
       172.16.0.0/16      192.168.1.2      1     0        RA      14
```

从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

(3)　配置 RIP 的版本。

```
# 在 RouterA 上配置 RIP-2。
    [RouterA] rip
    [RouterA-rip-1] version 2
    [RouterA-rip-1] quit
# 在 RouterB 上配置 RIP-2。
    [RouterB] rip
    [RouterB-rip-1] version 2
    [RouterB-rip-1] quit
# 在 RouterC 上配置 RIP-2。
    [RouterC] rip
    [RouterC-rip-1] version 2
    [RouterC-rip-1] quit
# 在 RouterD 上配置 RIP-2。
```

```
[RouterD] rip
[RouterD-rip-1] version 2
[RouterD-rip-1] quit
```

4) 验证配置结果

```
# 查看 RouterA 的 RIP 路由表。
[RouterA] display rip 1 route
    Route Flags: R - RIP
            A - Aging, S - Suppressed, G - Garbage-collect
-----------------------------------------------------------------------
 Peer 192.168.1.2  on GigabitEthernet1/0/0
     Destination/Mask        Nexthop      Cost   Tag    Flags   Sec
       10.1.1.0/24         192.168.1.2      1      0      RA      32
       172.16.1.0/24       192.168.1.2      1      0      RA      32
```

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。

2. RIP 与 BFD 联动

双向转发检测 BFD (Bidirectional Forwarding Detection)是一种用于检测邻居路由器之间链路故障的检测机制，它通常与路由协议联动，通过快速感知链路故障并通告使得路由协议能够快速地重新收敛，从而减少由于拓扑变化导致的流量丢失。

假设有如图 1-22 所示的网络拓扑结构，RouterA、RouterB 通过二层交换机 switch 互联，在设备上运行 RIP 协议来建立路由，同时使能允许 RIP 在双方接口上关联 BFD 应用。在 RouterB 和二层交换机 switch 之间的链路发生故障后，BFD 能够快速检测并通告 RIP 协议，触发协议快速收敛。

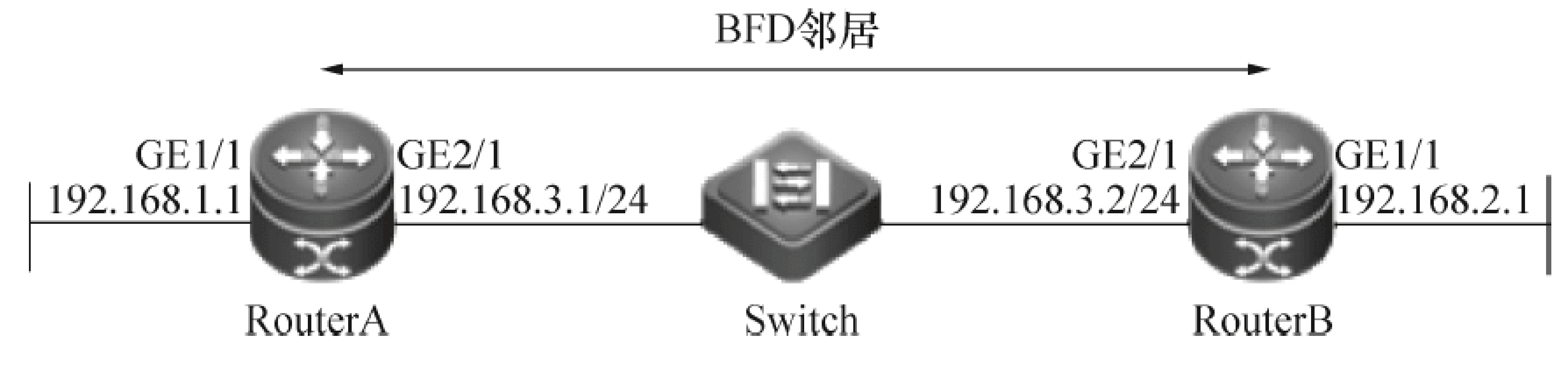



图 1-22 网络拓扑结构

Router A 配置如下：

(1) 配置 RIP 路由

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#ip ref
RSR-A(config-GigabitEthernet 2/1)#ip address 192.168.3.1 255.255.255.0
RSR-A(config)#interface gigabitEthernet 1/1

RSR-A(config-GigabitEthernet 1/1)#ip ref
RSR-A(config-GigabitEthernet 1/1)#ip address 192.168.1.1 255.255.255.0
RSR-A(config-router)#  router rip
RSR-A(config-router)#  version 2
RSR-A(config-router)#  network 192.168.3.0
```

```
RSR-A(config-router)#  network 192.168.1.0
```

(2) 配置 RIP 与 BFD 联动

```
RSR-A(config)#interface gigabitEthernet 2/1
RSR-A(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
//配置 BFD 时间参数，该命令同时启用了接口的 BFD 功能，因此必须配置；这里的 500/500/3 为推荐配置，间隔 500ms 发送一个探测报文，连续 3 个没收到回应宣告链路失败
RSR-A(config-GigabitEthernet 2/1)#no bfd echo
//推荐配置为该模式(ctrl 模式)，默认是 bfd echo 模式；和友商对接更是推荐 ctrl 模式，否则可能对接不起来
RSR-A(config-GigabitEthernet 2/1)#ip rip bfd
//在对应的接口开启 RIP 与 BFD 联动功能
```

Router B 配置如下：

(1) 配置 RIP 路由

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#ip ref
RSR-B(config-GigabitEthernet 2/1)#ip address 192.168.3.2 255.255.255.0
RSR-B(config)#interface gigabitEthernet 1/1
RSR-B(config-GigabitEthernet 1/1)#ip ref
RSR-B(config-GigabitEthernet 1/1)#ip address 192.168.2.1 255.255.255.0
RSR-B(config-router)#  router rip
RSR-B(config-router)#  version 2
RSR-B(config-router)#  network 192.168.3.0
RSR-B(config-router)#  network 192.168.2.0
```

(2) 配置 RIP 与 BFD 联动

```
RSR-B(config)#interface gigabitEthernet 2/1
RSR-B(config-GigabitEthernet 2/1)#bfd interval 500 min_rx 500 multiplier 3
RSR-B(config-GigabitEthernet 2/1)#no bfd echo
RSR-B(config-GigabitEthernet 2/1)#ip rip bfd
```

### 3. 配置 IS-IS 协议

中间系统到中间系统 IS-IS(Intermediate System to Intermediate System)属于内部网关协议 IGP(Interior Gateway Protocol)，用于自治系统内部。为了支持大规模的路由网络，IS-IS 在自治系统内采用骨干区域与非骨干区域两级的分层结构。一般来说，将 Level-1 路由器部署在非骨干区域，Level-2 路由器和 Level-1-2 路由器部署在骨干区域。每一个非骨干区域都通过 Level-1-2 路由器与骨干区域相连。

IS-IS 是一种链路状态路由协议，每一台路由器都会生成一个 LSP，它包含了该路由器所有启用 IS-IS 协议接口的链路状态信息。通过跟相邻设备建立 IS-IS 邻接关系，互相更新本地设备的 LSDB，可以使得 LSDB 与整个 IS-IS 网络的其他设备的 LSDB 实现同步。然后根据 LSDB 运用 SPF 算法计算出 IS-IS 路由。如果此 IS-IS 路由是到目的地址的最优路由，则此路由会下发到 IP 路由表中，并指导报文的转发。

其相关命令如表 1-2 所示。

表 1-2　IS-IS 的相关命令

| 命　令 | 功　能 |
|---|---|
| isis [process-id] | 创建 IS-IS 进程并进入 IS-IS 视图 |
| Isis circuit-level[level-1\|level-1-2\|level-2] | 设置接口的 Level 级别，默认情况下，接口的 Level 级别为 level-1-2 |
| Network-entity net | 设置网络实体名称 |
| Net | 格式为 x…x.xxxx.xxxx.xxxx.00，前面的“x…x”是区域地址，中间的 12 个“x”是路由器的 System ID，最后的“00”是 SEL |
| Isis enable[process-id] | 指定 IS-IS 的进程号，默认为 1，IS-IS 将通过该接口建立邻居、扩散 LSP 报文 |
| Display isis peer | 查看 IS-IS 的邻居信息 |
| Display isis route | 查看 IS-IS 的路由信息 |

4. 配置 OSPF 协议

开放最短路径优先协议是重要的路由选择协议，它是一种链路状态路由选择协议，是由 Internet 工程任务组开发的内部网关路由协议，用于在单一自治系统内决策路由。

链路是路由器接口的另一种说法，因此，OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。下面分别介绍 OSPF 协议的相关要点。

(1) 自治系统。自治系统包括一个单独管理实体下所控制的一组路由器，OSPF 是内部网关路由协议，工作于自治系统内部。

(2) 链路状态。所谓链路状态，是指路由器接口的状态，例如 Up、Down、IP 地址、网络类型、链路开销以及路由器和它邻接路由器间的关系。链路状态信息通过链路状态通告(Link State Advertisement，LSA)扩散到网络上的每台路由器，每台路由器根据 LSA 信息建立一个关于网络的拓扑数据库。

(3) 最短路径优先算法。OSPF 协议使用最短路径优先算法，利用从 LSA 通告得来的信息计算到达每一个目标网络的最短路径，以自身为根生成一棵树，包含了到达每个目的网络的完整路径。

(4) 路由器标识。OSPF 的路由标识是一个 32 位的数字，它在自治系统中被用来唯一地识别路由器。默认使用最高回送地址，若回送地址没有被配置，则使用物理接口上最高的 IP 地址作为路由器标识。

(5) 邻居和邻接。OSPF 在相邻路由器间建立邻接关系，使它们交换路由信息。邻居是指共享同一网络的路由器，并使用 Hello 包来建立和维护邻居路由器间的邻接关系。

(6) 区域。在 OSPF 网络中使用区域(Area)为自治系统分段。OSPF 是一种层次化的路由选择协议，区域 0 是一个 OSPF 网络中必须具有的区域，也称为主干区域，其他所有区域要求通过区域 0 互联到一起。

其相关命令及说明如表 1-3 所示。

表 1-3　OSPF 的相关命令

| 命　令 | 功　能 |
| --- | --- |
| ospf[process-id\|router-id router-id\|vpn-instance vpn-instance-name] | 启动 OSPF 进程，进入 OSPF 视图 |
| area area-id | 创建并进入 OSPF 区域视图 |
| network ip-address wildcard-mask | 配置区域所包含的网段 |
| display ospf peer | 查看 OSPF 邻居信息 |
| display ospf routing | 查看 OSPF 路由信息 |

5. 配置 BGF 协议

边界网关协议 BGP(Border Gateway Protocol)是一种实现自治系统 AS (Autonomous System)之间的路由可达，并选择最佳路由的距离矢量路由协议。它具有以下特点。

(1) 实现自治系统间通信网络的信息可达，BGP 允许一个 AS 向其他 AS 通告其内部网络的可达性信息，或者是通过该 AS 可达的其他网络的路由信息。

(2) 多个 BGP 路由器之间的协调，如果在一个自治系统内部有多个路由器分别使用 BGP 与其他自治系统中对等路由器进行通信，则通过协调使这些路由器保持路由信息的一致性。

(3) BGP 支持基于策略的路径选择，可以为域内和域间的网络可达性配置不同的策略。

(4) BGP 只需要在启动时交换一次完整信息，不需要在所有路由更新报文中传送完整的路由数据库信息，后续的路由更新报文只通告网络的变化信息，避免网络变化使得信息量大幅增加。

(5) 在 BGP 通告目的网络的可达性信息时，除了处理指定目的网络的下一跳信息之外，通告中还包括了通路向量，即去往该目的网络时需要经过的 AS 的列表，使接受者能够清楚了解去往目的网络的通路信息。

除了以上这些，BGP 允许发送方把路由信息聚集在一起，用一个条目来表示多个相关的目的网络，以节约网络带宽。允许接收方对报文进行鉴别，以验证发送方的身份等多个特点。

BGP 在不同自治系统(AS)之间进行路由转发，分为 EBGP 和 IBGP 两种情况。EBGP 外部边界网关协议，用于在不同的自治系统间交换路由信息。IBGP 内部边界网关协议，用于向内部路由器提供更多信息。

其相关命令及说明如表 1-4 所示。

表 1-4　BGP 的相关命令

| 命　令 | 功　能 |
| --- | --- |
| bgp{as—number-plain\|as-number-dot} | 启动 BGP，指定本地 AS 编号，并进入 BGP 视图 |
| router-id ipv4-address | 配置 BGP 的 Router ID |
| peer{ipv4-address\|ipv6-address}as-number {as-number-plain\|as-number-dot} | 创建 BGP 对等体 |
| ipv4-family {unicast\|muliticast} | 进入 IPv4 地址地址族视图 |
| import-route direct | 管理 IP 所在的网段路由，并引入 RIP 路由表 |

## 1.4.2 典型例题分析

**例** 阅读以下技术说明，根据要求回答问题 1 至问题 4。

**【说明】**

图 1-23 是 VLAN 配置的拓扑结构示意图。

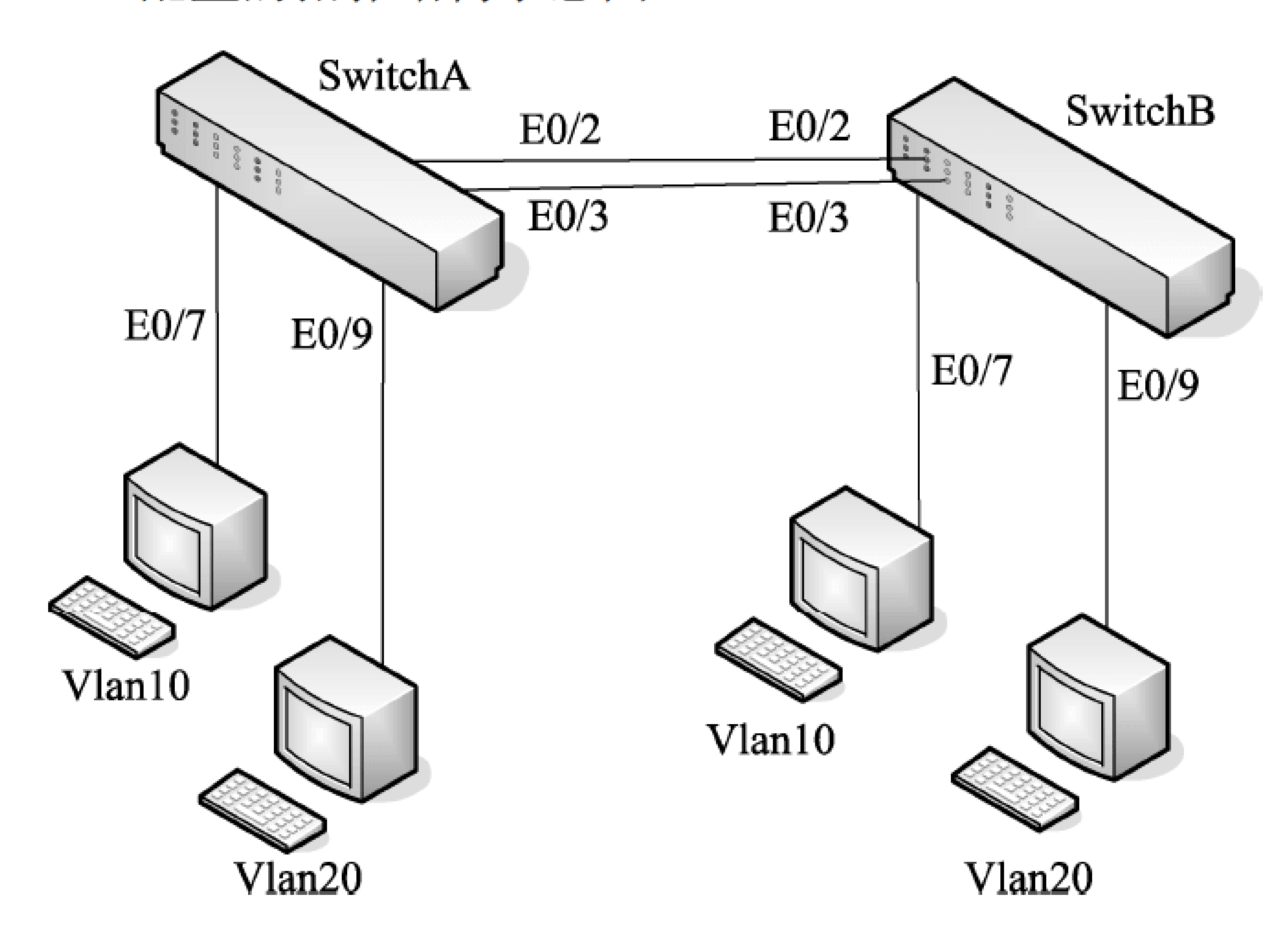



图 1-23 某 VLAN 配置的拓扑结构

**【问题 1】**(5 分)

请阅读下列关于 SwitchA 的配置信息，并在(1)～(5)处解释相应语句的作用。

```
SwitchA> enable                        //进入特权模式
Switch# config terminal                //进入配置模式
Switch(config)# hostname SwitchA       ____(1)____
SwitchA(config)# end
SwitchA#
SwitchA# vlan database                 ____(2)____
SwitchA(valn)# vtp server              ____(3)____
SwitchA(valn)# vtp domain vtpserver    ____(4)____
SwitchA(valn)# vtp pruning             ____(5)____
SwitchA(valn)# exit                    //退出 VLAN 配置模式
```

**【问题 2】**(2 分)

下面是交换机完成 Trunk 的部分配置，请根据题目要求完成下列配置。

```
SwitchA(config)# interface f0/3                  //进入端口 3 配置模式
SwitchA(config-if)# switchport____(6)____        //设置当前端口为 Trunk 模式
SwitchA(config-if)# switchport trunk ____(7)____ //设置允许所有 Vlan 通过
SwitchA(config-if)# exit
SwitchA(config)# exit
Switch#
```

【问题 3】(4 分)

下面是交换机完成端口配置的过程，请根据题目要求完成下列配置。

```
Switch(config)# interface f0/7          //进入端口 7 配置模式
Switch(config-if)# ____(8)____          //设置端口为静态 VLAN 访问模式
Switch(config-if)# ____(9)____          //把端口 7 分配给 VLAN10
Switch(config-if)# exit
Switch(config)# exit
```

【问题 4】(2 分)

基于交换机端口的 VLAN 划分方法属于 (10) 。

A.　动态 VLAN 实现方式　　　　B.　静态 VLAN 实现方式

【问题 5】(2 分)

在 VLAN 中，STP 是指 (11) 协议，VTP 是指 (12) 协议。

分析：

【问题 1】

本题要求考生掌握 VTP 配置的命令解释。对于(1)空缺，由它所在命令行的交换机配置模式“Switch(config)#”和下一行“SwitchA(config)#”的不同可知，配置语句 hostname SwitchA 的作用是将该交换机的主机名修改为 SwitchA；对于(2)空缺，由它所在命令行的交换机配置模式“SwitchA#”和下一行“SwitchA(valn)#”的不同可知，配置语句 vlan database 的作用是进入该交换机的 VLAN 配置子模式；在交换机的 VLAN 配置子模式中，(3)空缺处的命令行的配置语句为 vtp server，其作用是设置该交换机的 VTP 模式为 Server 模式；(4)空缺处所在命令行的配置语句为 vtp domain vtpserver，其作用是设置该交换机的 VTP 管理域名为 vtpserver；(5)空缺处所在命令行的配置语句为 vtp pruning，其作用是启动该交换机的 VTP 修剪功能。

【问题 2】

本题要求考生掌握交换机 VLAN Trunk 端口配置的实践操作过程。解答思路如下。

①　跨交换机的同一 VLAN 内的数据经过 Trunk 线路进行交换，在默认情况下 Trunk 允许所有的 VLAN 通过。

②　配置语句 interface f0/3 使得交换机从配置模式进入到快速以太网端口 3 的配置模式。根据(6)空缺处所在命令行后面的解释信息“设置当前端口为 Trunk 模式”可知，(6)空缺处完整的配置语句是 switchport mode trunk。

③　根据(7)空缺处所在命令行后面的解释信息“设置允许所有 Vlan 通过”可知，(7)空缺处完整的配置语句是 switchport trunk allowed vlan all。

【问题 3】

本题要求掌握将交换机某端口添加到某个 VLAN 中的实践操作过程。

由于交换机出厂配置的工作状态是服务器模式，系统自动创建一个 VLAN(即 VLAN1)默认将所有的端口都归属到这个 VLAN 内。因此，在交换机中配置 VLAN 时，VLAN1 不能被创建、删除或重命名。

在基于端口的 VLAN 划分中，交换机上的每一个端口允许以 access、multi、trunk 这 3

种模式划入 VLAN 中。其中，对于 access 模式，端口仅能属于一个 VLAN，只能接受没有封装的帧；对于 multi 模式，端口可以同时属于多个 VLAN，但只能接受没有封装的帧；对于 trunk 模式，该端口可以接收包含所属 VLAN 信息的封装帧，同时允许不同设备的相同 VLAN 通过 trunk 互连。

配置语句 interface f0/7 使得交换机从配置模式进入到快速以太网端口 7 的配置子模式。根据(8)空缺处所在命令行后面的解释信息“设置端口为静态 VLAN 访问模式”可知，(8)空缺处所填写的配置语句应是 switchport mode access。

根据(9)空缺处所在命令行后面的解释信息“把端口 7 分配给 VLAN10”可知，(9)空缺处所填写的配置语句应是 switchport access vlan10。

**【问题 4】**

这是一道要求掌握静态和动态 VLAN 基本知识及其特点的问答题。本题所涉及的知识点如下。

静态 VLAN 划分是创建 VLAN 最常用的方法。形成静态 VLAN 的过程是将交换机端口强制性地分配给某个 VLAN 的过程，即先在交换机上建立 VLAN，指定其基本参数(如 VTP 域、VLAN ID 等)，然后将交换机的每个端口分配给相应的 VLAN。在没有人为地修改该端口之前，该端口一直属于某一个 VLAN。不管是哪种网络设备接入该端口，它所归属的 VLAN 都不会改变。这种划分方式是基于端口来划分的，容易实现和监视且比较安全，但是设置烦琐(每个端口都要设置)，并且 VLAN 的变化不灵活。如果想要改变某个端口的 VLAN，必须手动修改交换机配置。基于交换机端口的 VLAN 划分方法属于静态 VLAN 实现方式。

动态 VLAN 的配置可以基于网络设备的 MAC 地址、IP 地址、应用协议来实现。在动态方式中，管理员必须先建立一个较复杂的数据库，如输入要连接的网络设备的 MAC 地址及相应的 VLAN 号。当网络设备连接到交换机端口时，交换机自动把这个网络设备所连接的端口分配给相应的 VLAN。实现动态 VLAN 时，一般使用管理软件来进行管理。这种划分方式的特点是：VLAN 的变化很灵活，初始化配置后就不用关心用户接入哪个具体端口，但是要维护一个全网的数据库表，而且每次新用户加入时都需要进行较复杂的手工配置，即初始化配置的工作量较大。

**【问题 5】**

这是一道要求掌握 STP 和动态 VTP 含义及其作用的简答题。本题所涉及的知识点如下。

在交换机配置中，生成树协议(STP)是一个既能够防止环路又能够提供冗余线路的二层管理协议。为了使交换网络正常运行，STP 网络上的任何两个终端之间只有一条有效路径，既能暂时切断网络中的环路，在网络的环路消失之后又能自动打开关闭的端口，从而保证网络不会中断。STP 使用生成树算法来求解无环路网络的最佳路径，使一些备用路径处于阻塞状态。大型交换网络中尤其是有多个 VLAN 的时候配置 STP 很重要。STP 操作对于终端来说是透明的，而终端不管它们是连在 VLAN 的一个部分还是多个部分。

VLAN 中继协议可以保持网络中 VLAN 配置的一致性，即在 VTP 域的某台交换机中增加、删除和调整 VLAN 时，VTP 会自动地把交换机的 VLAN 变化信息向网络中其他的交换机广播，使得整个网络中同一个 VTP 域中的所有交换机同步地知道网络中其他交换机的 VLAN 变化信息，从而保持全网中交换机 VLAN 信息的自动同步。同时，VTP 还可以减少

那些可能导致安全问题的配置。

答案：

【问题 1】

(1) 修改主机名为 SwitchA

(2) 进入 VLAN 配置子模式

(3) 设置本交换机为 Server 模式

(4) 设置 VTP 管理域名为 vtpserver

(5) 启动修剪功能

【问题 2】

(6) mode trunk　　(7) allowed vlan all

【问题 3】

(8) switchport mode access　　(9) switchport access vlan 10

【问题 4】

(10) B

【问题 5】

(11) 生成树　　(12) VLAN 中继

## 1.4.3　同步练习

阅读以下技术说明，根据要求回答问题 1 至问题 4。

【说明】

某单位内部网络拓扑结构如图 1-24 所示。

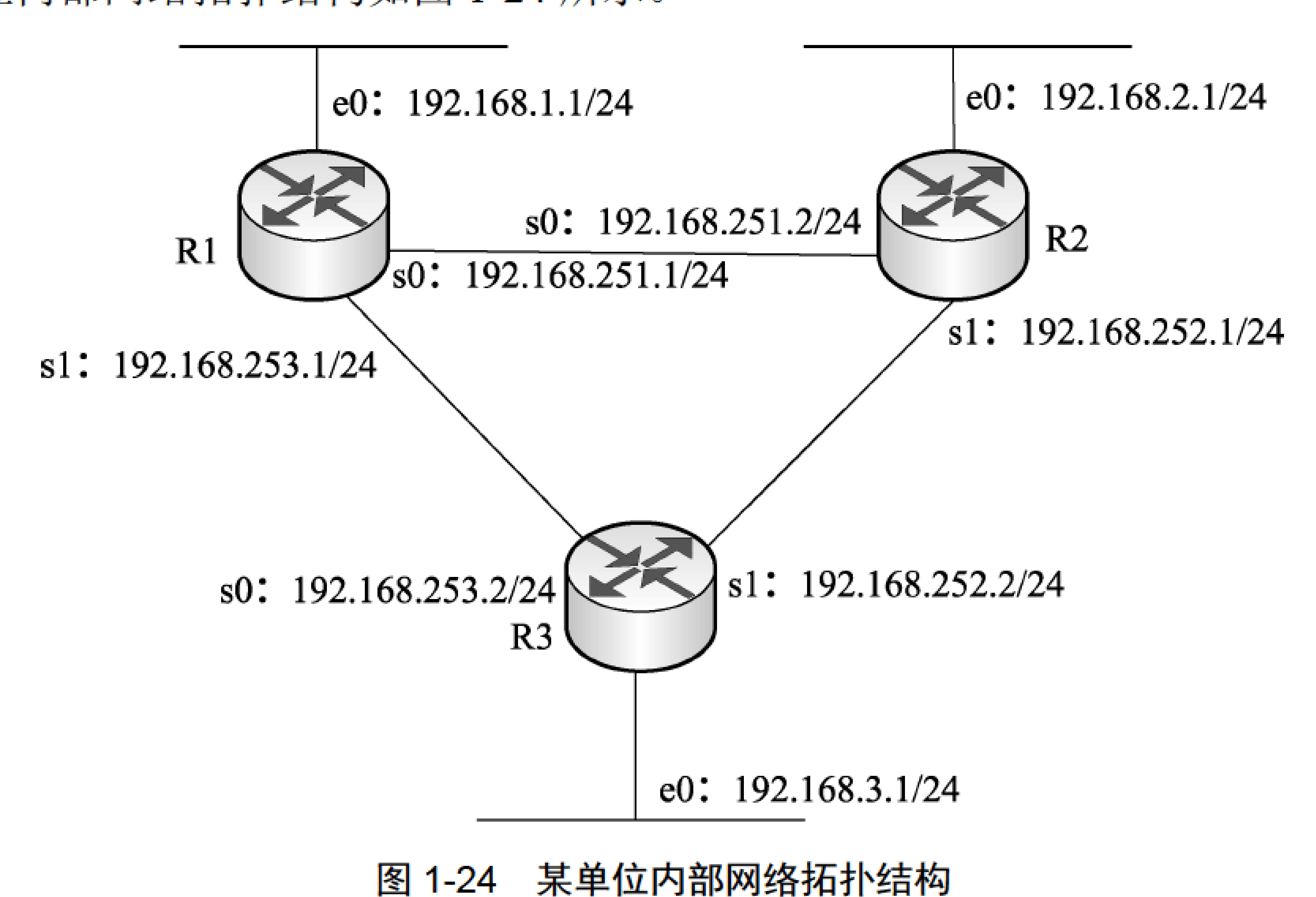



图 1-24　某单位内部网络拓扑结构

【问题 1】(2 分)

路由器第一次设置时，必须通过 Console 端口连接运行终端仿真软件的计算机进行配

置，此时终端仿真程序设置的波特率为____(1)____b/s。

**【问题 2】**(4 分)

路由器有多种配置模式，请根据以下命令提示信息，判断路由器处于何种配置模式下。

```
Router(Config) #                ____(2)____
Router >                        ____(3)____
Router #                        ____(4)____
Router(Config-if) #             ____(5)____
```

**【问题 3】**(5 分)

以下是路由器 R1 的部分配置，请完成其配置，或者解释配置命令的含义。

```
R1(Config) #interface Fastethernet0
R1(Config-if) # ip address ____(6)____ ____(7)____
R1(Config-if) # ____(8)____
!
R1(Config) #interface serial0
R1(Config-if) # ip address ____(9)____        ____(10)____
```

**【问题 4】**(4 分)

为保证路由器的安全，网络管理员进行了以下设置，请在(11)～(13)处填写对应行语句的作用。

```
outer(Config) #no ip http server                        ____(11)____
outer(Config) #snmp-server community admin RW           ____(12)____
outer(Config) #access-list permit 192.168.5.1
Router(Config) #line con 0
Router(Config-line) #transport input none
Router(Config-line) #login local
Router(Config-line) #exec-timeout 5 0
Router(Config-line) #access-class 1 in                  ____(13)____
```

## 1.4.4 同步练习参考答案

**【问题 1】**

(1) 9600

**【问题 2】**

(2) 全局配置模式　　(3) 用户模式

(4) 特权模式　　(5) 接口配置模式

**【问题 3】**

(6) 192.168.1.1　　(7) 255.255.255.0　　(8) no shutdown

(9) 192.168.251.1　　(10) 255.255.255.0

**【问题 4】**

(11) 禁止以非加密的 HTTP 方式访问路由器，或路由器禁止 HTTP 服务

(12) 配置路由器具有读写权限的团体名为 admin

(13) 设置 ACL 允许 192.168.5.1 访问 Console0 端口

# 1.5　综合布线

## 1.5.1　考点辅导

### 1.5.1.1　综合布线系统概述

1. 综合布线系统的概念

综合布线系统(Premises Distribution System，PDS)是专为通信与计算机网络而设计的，它可以满足各种通信与计算机信息传输的要求，是为具有综合业务需求的计算机数据网开发的。

综合布线系统具体的应用对象主要是通信和数据交换，即语音、数据、传真、图像信号。综合布线系统是一套综合系统，它可以使用相同的线缆、配线端子板、插头及模块插孔，解决传统布线存在的兼容性问题。综合布线系统是智能化大厦工程的重要组成部分，是智能化大厦传送信息的神经中枢。

2. 综合布线系统的特点

与传统布线系统相比，综合布线系统具有兼容性、开放性、灵活性、可靠性、经济性、先进性等特点。

1)　兼容性

兼容性是指其设备可以用于多种系统。它将语音、数据信号的配线统一设计规划，采用统一的传输线、信息插接件等把不同信号综合到一套标准布线系统中，同时该系统比传统布线系统简捷很多，不存在重复投资，可以节约大量资金。

2)　开放性

综合布线系统由于采用开放式体系结构，符合国际标准，对现有著名厂商的硬件设备均是开放的，对通信协议也同样是开放的。

3)　灵活性

综合布线系统中每条线路均可传送语音、传真和数据，所有系统内的设备(计算机、终端、网络集线器、集线器或中心集线器、电话、传真)的开通及变动无须改变布线，只要在设备间或管理间做相应的跳线操作即可。

4)　可靠性

综合布线系统全部使用物理星型拓扑结构，任何一条线路有故障都不会影响其他线路，从而提高了可靠性。各系统采用同一传输介质，互为备用，又提高了备用冗余。

5)　经济性

综合布线系统设计信息点时要求按规划容量留有适当的发展容量，因此，就整体布线系统而言，按规划设计所做的经济分析表明，综合布线系统会比传统布线系统的性价比更优，后期运行维护及管理费也会下降。

6)　先进性

为了适应数据传递、语音及多媒体技术的发展，综合布线系统采用双绞线与光纤混合

布置方式进行布线。

3. 综合布线标准

综合布线标准有以下几种。

- 《建筑与建筑群综合布线系统工程设计规范》(国家标准 GB 30511—2000)。
- 《建筑与建筑群综合布线系统工程施工和验收规范》(国家标准 GB 30512—2000)。
- 《大楼通信综合布线系统第一部分总规范》(YD/T 926.1—2001)。
- 《大楼通信综合布线系统第二部分综合布线用电缆光纤技术要求》(YD/T 926.2—2001)。
- 《大楼通信综合布线系统第三部分综合布线用连接硬件技术要求》(YD/T 926.3—2001)。
- 《商用建筑通信布线标准》(北美标准 ANSI/TIA/EIA 568B)。
- 《信息技术——用户通用布线系统》(第 2 版)(国际标准 ISO/IEC 11801)。
- 《国际电子电气工程师协会：CSMA/CD 接口方法》(IEEE 802.3)。

4. 综合布线系统的构成

综合布线系统由 6 个子系统组成，即水平子系统、垂直子系统、工作区子系统、管理子系统、设备间子系统及建筑群子系统。大型布线系统需要用铜介质和光纤介质将 6 个子系统集成在一起。

(1) 水平子系统。它由信息插座、配线电缆或光纤、配线设备和跳线等组成，又称为配线子系统。

(2) 垂直子系统。它由配线设备、干线电缆或光纤、跳线等组成，又称为干线子系统。

(3) 工作区子系统。它需要终端设备的独立区域。

(4) 管理子系统。它是针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

(5) 设备间子系统。它是安装各种设备的场所。对综合布线而言，还包括安装的配线设备。

(6) 建筑群子系统。它由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

### 1.5.1.2 综合布线系统设计

1. 系统设计原则

在进行综合布线系统设计时通常应遵循以下原则。

(1) 采用模块化设计，易于在配线上扩充和重新组合。

(2) 采用星型拓扑结构，从而使系统扩充和故障分析变得十分容易。

(3) 应满足通信自动化与办公自动化的需要，即满足语音与数据网络的广泛要求。

(4) 确保任何插座互连主网络，尽量提供多个冗余互连信息点插座。

(5) 适应各种符合标准的品牌设备互联入网，满足当前和将来网络的要求。

(6) 电缆的铺设与管理应符合综合布线系统的设计要求。

2. 工作区子系统设计

工作区子系统提供从水平子系统的信息插座到用户工作站设备之间的连接，它包括工

作站连线、适配器和扩展线等。

一部电话机或一台计算机终端设备的服务面积可按 8～10m$^2$ 设置，也可按用户要求设置。采用标准信息插座，型号为 RJ-45，采用 8 芯连线，全部按标准制造，符合 ISDN 标准。在 RJ-45 插座内不仅可以插入数据通信通用的 RJ-45 接头，也可以插入电话机专用的 RJ-12 插头。

信息插座通常有 3 种安装形式，即安装于地面上、安装于分隔板上及安装于墙上。如果安装于墙上，信息插座应放置在距地面 30～50cm 处。

### 3. 水平子系统设计

水平子系统是将垂直子系统线路延伸到用户工作区，由工作区的信息插座、信息插座至楼层配线设备(FD)的配线电缆或光纤、楼层配线设备和跳线等组成。

水平子系统的设计应按以下要求进行。

(1) 水平子系统一般应使用 20 年左右，通常采用管线铺设，这也对双绞线的性能和质量提出了更高的要求。

(2) 进行网络布线时应考虑未来的发展(信息点冗余及网络带宽的需求)。

(3) 水平子系统采用 4 对双绞线，通常在超 5 类和 6 类之间选择，在高速率应用场合宜采用光缆。

(4) 根据整个综合布线系统的要求，应在交换间或设备间的配线设备上进行连接，以构成电话、数据传输设备并进行管理，配线电缆宜采用双绞线。电缆长度应在 90m 以内。

### 4. 垂直子系统设计

垂直子系统主要用于连接各层配线室，并连接主配线室。其设计要求如下。

(1) 为安装和固定垂直子系统的电缆，要求建筑物竖井中应立有金属线槽，且每隔 2m 焊一根粗钢筋。

(2) 竖井中的线槽与各层配线室之间应有金属线槽连通。

(3) 垂直子系统采用的介质大多数为双绞线电缆和光纤。

### 5. 管理子系统设计

管理子系统由交连、互连配线架组成，为连接其他子系统提供手段。其设计要求如下。

(1) 根据信息点的数量，对于信息点不是很多的楼层，为便于管理，几个楼层可共用一个子配线间；对于有较多信息点的楼层，一个楼层设置一个配线间。

(2) 配线间的位置可选在弱电井附近的房间内。配线室设标准机柜，用于安装配线架(双绞线、光纤)和计算机网络通信设备。

### 6. 设备间子系统设计

设备间子系统(主配线间)由设备间中的电缆、连接器和相关支撑硬件组成，它把公共系统中的各种不同设备互连起来。该子系统将中继线交叉连接处和布线交叉处与公共系统设备(如 PBX)连接起来。其设计要求如下。

(1) 通常主配线架设置在程控机房内，用于垂直光缆和 PABX 的连接。建议采用 QCBIX 系列配线架，可充分满足语音通信的要求。

(2) 通常计算机网络主配线架设在网管中心，使用光纤配线架，用来连接来自各分配

线间的光纤，并通过光纤跳线和计算机网络中心交换机相连。光纤配线架可直接安装在标准的19in机柜内，用于主干光纤和网络设备的连接，十分易于管理。

(3) 对于设备间的建设应满足一定的要求，如室温、湿度、地板负重能力、消防、电源及UPS等。

7. 建筑群子系统设计

建筑群子系统应由连接各建筑物之间的综合布线缆线、建筑群配线设备(CD)和跳线等组成。其设计要求如下。

(1) 建筑物间的缆线宜采用地下管道或电缆沟的铺设方式。

(2) 建筑物群干线电缆、光缆、公用网和专用网电缆、光缆(包括天线馈线)进入建筑物时，都应设置引入设备，并在适当位置转换为室内电缆、光纤。引入设备还包括必要的保护装置。引入设备宜单独设置房间，如条件合适也可与BD或CD合设。引入设备的安装应符合相关规定。

(3) 建筑群和建筑物的干线电缆、主干光缆布线的交接不应多于两次。

(4) 从楼层配线架(FD)到建筑群配线架之间只应通过一个建筑物配线架(BD)。

8. 管线设计

综合布线系统中管线设计通常采用两种方案，即装配式槽形电缆桥架和地面线槽走线。

9. 电气防护、接地及防火设计

综合布线系统应根据环境条件选用相应的缆线和配线设备，或采取防护措施，并应符合下列规定。

(1) 当综合布线区域内存在干扰或用户对电磁兼容性有较高要求时，宜采用屏蔽缆线和屏蔽配线设备进行布线，也可采用光纤系统。采用屏蔽布线系统时，所有屏蔽层应保持连续性。

(2) 综合布线系统采用屏蔽措施时，必须有良好的接地系统。

(3) 当电缆从建筑物外面进入建筑物时，电缆的金属护套或光纤的金属件均应有良好的接地，同时要采用过压、过流保护措施，并符合相关规定。

(4) 根据建筑物的防火等级和对材料的耐火要求，综合布线应采取相应的措施。

(5) 当综合布线线路上存在干扰源且不能满足最小净距要求时，宜采用金属管线进行屏蔽。综合布线电缆与附近可能产生高频电磁干扰的电动机、电力变压器等电气设备之间应保持必要的间距。墙上铺设的综合布线电缆、光纤及管线与其他管线应保持适当的间距。

### 1.5.1.3 综合布线系统的性能指标及测试

1. 双绞线系统的测试元素及标准

1) 连接图

连接图用于显示双绞线的详细情况。连接图测试通常是一个布线系统的最基本测试，因而对于3～5类布线系统都要求进行连接图测试。

2) 线缆长度

3～5类布线系统都要求对线缆长度进行准确测试。对线缆长度要求如下：基本回路线

缆长度不大于 94m(包括测试跳线)，通道回路线缆长度不大于 100m(包括设备跳线和快接式跳线)。

3)　衰减

由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素，造成信号沿链路传输损失的能量，称为衰减。衰减是针对“基本回路”/“通道回路”信号损失程度的量度。最坏线对的衰减应小于“基本回路”/“通道回路”允许的最大衰减值。

4)　近端串音(NEXT)衰减

电磁波从一个传输回路(主串回路)串入另一个传输回路(被串回路)的现象称为串音，能量从主串回路串入回路时的衰减称为串音衰减。在 UTP 布线系统中，近端串音为主要的影响因素。布线系统都应通过 NEXT 衰减的测试，而且 NEXT 衰减的测试必须从两个方向进行，也就是双向测试。

5)　回波损耗

回波损耗(Return Loss，RL)是电缆传输系统的一个重要参数。该参数定义为开始输入给信号传输系统的信号与信号源接收到的反射信号的功率之比。不良连接器、操作不当或不正确的线缆拖拉和安装方式都会使线缆产生变形，从而引起回波损耗问题的发生。

2.　光缆布线系统的测试元素及标准

(1)　波长窗口参数。综合布线系统光纤波长窗口的各项参数应符合表 1-5 的规定。

**表 1-5　光纤波长串口参数**

| 光纤模式 | 波长下限/nm | 波长上限/nm | 基准试验波长/nm | 谱线最大宽度/nm |
|---|---|---|---|---|
| 多模 | 790 | 910 | 850 | 50 |
| 多模 | 1285 | 1330 | 1300 | 150 |
| 单模 | 1288 | 1339 | 1310 | 10 |
| 单模 | 1525 | 1575 | 1550 | 10 |

(2)　光缆布线链路的最大衰减限值。综合布线系统的光纤布线链路的衰减限值应符合表 1-6 的规定。

**表 1-6　光纤布线链路的最大衰减限值**

| 应用类别 | 链路长度/m | 多模衰减值/dB | | 单模衰减值/dB | |
|---|---|---|---|---|---|
| | | 850/nm | 1300/nm | 1310/nm | 1550/nm |
| 水平子系统 | 100 | 2.5 | 2.2 | 2.2 | 2.2 |
| 垂直子系统 | 500 | 3.9 | 2.6 | 2.7 | 2.7 |
| 建筑群子系统 | 1500 | 7.4 | 3.6 | 3.6 | 3.6 |

(3)　光回波损耗限值。综合布线系统光纤布线链路任一接口的光回波损耗限值应符合表 1-7 的规定。

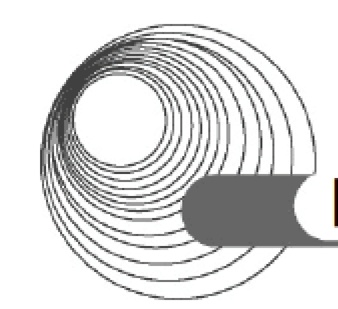



表 1-7　最小的光回波损耗限值

| 光纤模式、标称波长/nm | 最小的光回波损耗限值/dB |
|---|---|
| 多模 850 | 20 |
| 多模 1300 | 20 |
| 单模 1310 | 26 |
| 单模 1550 | 26 |

3. 测试环境

(1) 测试条件。综合布线最小模式带宽测试现场应无产生严重电火花的电焊、电钻和产生强磁干扰的设备作业，被测综合布线系统必须是无源网络、无源通信设备。

(2) 测试温度。综合布线测试现场温度在 20～30℃之间，湿度宜在 30%～80%之间，由于衰减指标的测试受测试环境温度影响较大，当测试环境温度超出上述范围时，需要按照有关规定对测试标准和测试数据进行修正。

(3) 测试仪表。按时域原理设计的测试仪均可用于综合布线现场测试，但测试仪的测量扫描步长要满足近端串扰指标测量精度的基本要求，能够在 0～250MHz 频率范围内提供各测试参数的标称值和阈值曲线，每测试一条链路时间不应大于 25s，且每条链路应具有一定的故障定位诊断能力，即具有自动、连续、单项选择测试的功能。

4. 测试流程

在开始测试之前应该认真了解布线系统的特点、用途，信息点的分布情况，确定测试标准。在选定测试仪后按下述程序进行。

(1) 测试仪测试前自检，确认仪表是正常的。
(2) 选择测试方式。
(3) 选择设置线缆类型及测试标准。
(4) 核准 NVP 值。核准 NVP 时使用缆长不短于 15m。
(5) 设置测试环境湿度。
(6) 根据要求选择“自动测试”或“单项测试”命令。
(7) 测试后存储数据并打印。
(8) 发生问题时修复后复测。
(9) 测试中出现“失败”后查找故障。

## 1.5.2　典型例题分析

**例 1**　阅读以下说明并回答问题，将解答填入答题纸对应的解答栏内。(2015 年 11 月下午试题一)

**【说明】**

某单位网络拓扑结构如图 1-25 所示，要求办公楼能与互联网物理隔离，所有汇聚交换机均采用三层交换机。

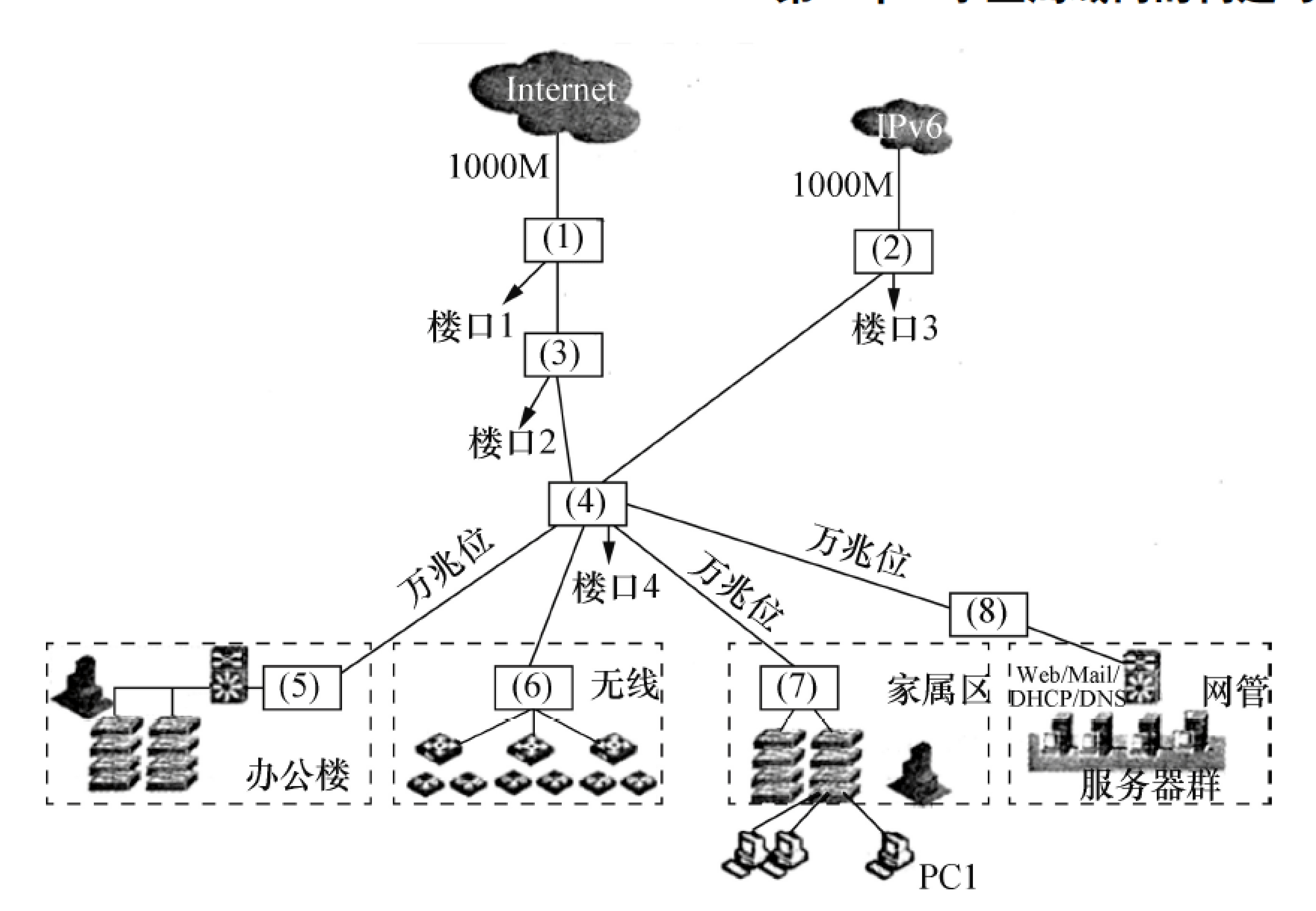



图 1-25　综合布线系统的构成

【问题 1】

请为图 1-23 中空缺处(1)～(8)选择合适设备(限选一次)。

(1)～(8)备选答案：

A．网闸　　B．汇聚交换机　　C．核心交换机

D．AP 控制器　　E．出口路由器　　F．IPv6 路由器

G．防火墙　　H．并发与流量控制器(采用桥接模式)

**分析**：本问题考查设备的选择。通常出口处均是路由器，IPv4(图中(1)处)与 IPv6(图中(2)处)出口处分别是出口路由器和 IPv6 路由器；并发与流量控制器通常放在路由器之后，交换主干之前，故(3)处为并发与流量控制器；(4)处是交换核心，故采用核心交换机；办公楼与互联网物理隔离，故(5)处为网闸；(6)处管理无线局域网接入，故为 AP 控制器；(7)处的汇聚交换机以及(8)处的防火墙较为明显。

**答案**：

【问题 1】

(1)　E　(2)　F　(3)　H　(4)　C

(5)　A　(6)　D　(7)　B　(8)　G

**例 2**　阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题二)

【说明】

某单位网络拓扑结构如图 1-26 所示，FTP 服务器的域名为 xhfip.SoftwareExam.com。

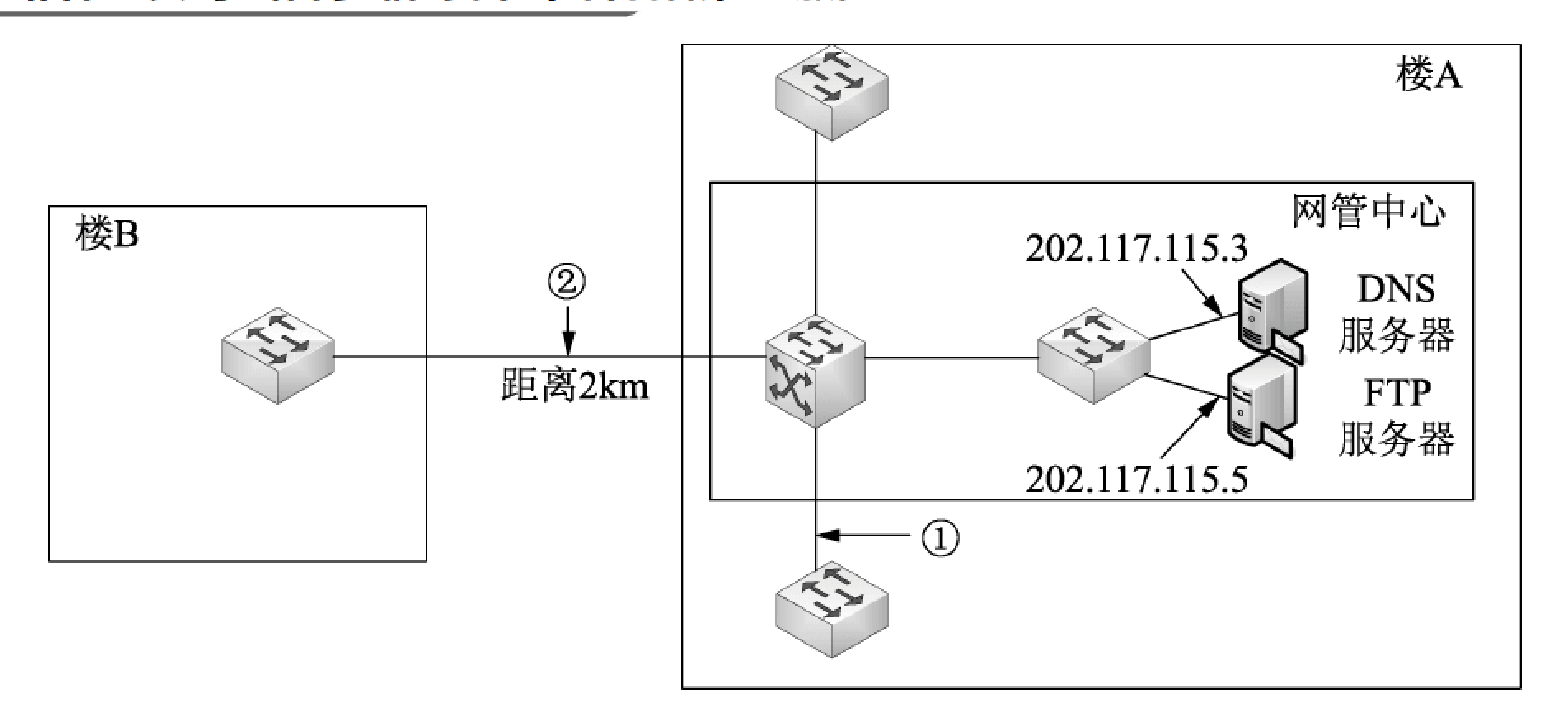



图 1-26　综合布线某单位网络拓扑结构

【问题 1】

在该单位综合布线时，连接楼 A 与楼 B 的布线子系统为__(1)__；楼 A 内网管中心服务器群至核心交换机的布线子系统为__(2)__。

(1)、(2)备选答案：

A. 水平子系统　　B. 垂直子系统　　C. 设备间子系统

D. 建筑群子系统　　E. 干线子系统　　F. 管理子系统

【问题 2】

图 1-24 中①的传输介质为__(3)__，②的传输介质为__(4)__。

(3)、(4)备选答案(限选一次)

A. 单模光纤　　B. 多模光纤

**分析：**

【问题 1】

综合布线系统由 6 个子系统组成，即建筑群子系统、设备间子系统、干线子系统、 管理子系统、配线子系统、工作区子系统。大型布线系统需要用铜介质和光纤介质部件将 6 个子系统集成在一起。

① 水平子系统(Horizontal Subsystem)：由信息插座、配线电缆或光纤、配线设备和跳线等组成。国内称之为配线子系统。

② 垂直子系统(Backbone Subsystem)：由配线设备、干线电缆或光纤、跳线等组成。国内称之为干线子系统。

③ 工作区子系统(WorkArea Subsystem)：为需要设置终端设备的独立区域。

④ 管理子系统(Administration Subsystem)：针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

⑤ 设备间子系统(Equipment Room Subsystem)：安装各种设备的场所，对综合布线而言，还包括安装的配线设备。

⑥ 建筑群子系统(Campus Subsystem)：由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

由此，题目中连接楼 A 与楼 B 的布线子系统为建筑群子系统；楼 A 内网管中心服务器

群至核心交换机的布线子系统为设备间子系统。

【问题 2】

图 1-24 中①处传输介质连接两个楼层，可选多模光纤，②处连接两个建筑物，且距离 2km，故传输介质为单模光纤。

答案：

【问题 1】

(1)　D　(2)　C

【问题 2】

(3)　B　(4)　A

## 1.5.3　同步练习

1．什么是综合布线？综合布线的特点是什么？综合布线系统由哪几个子系统构成？

2．在综合布线中，对双绞线进行测试，主要测试哪些元素？

3．在综合布线中，对光纤进行测试，主要测试哪些元素？

## 1.5.4　同步练习参考答案

1．综合布线系统(Premise Distribution System，PDS)是专为通信与计算机网络而设计的，它可以满足各种通信与计算机信息传输的要求，是为具有综合业务需求的计算机数据网开发的。

与传统布线系统相比较，综合布线系统具有兼容性、开放性、灵活性、可靠性、经济性、先进性的特点。

综合布线系统由 6 个子系统组成，即水平子系统、垂直子系统、工作区子系统、管理子系统、设备间子系统及建筑群子系统。

2．连接图、线缆长度、衰减、近端串音衰减、回波损耗。

3．波长窗口、衰减、回波损耗。

# 1.6　IP 地址及其规划

## 1.6.1　考点辅导

### 1.6.1.1　IP 地址基础

Internet 是由不同物理网络互联而成的，不同网络之间实现计算机的相互通信必须有相应的地址标识，这个地址标识称为 IP 地址。图 1-27 所示为 IP 地址的组成与表示。

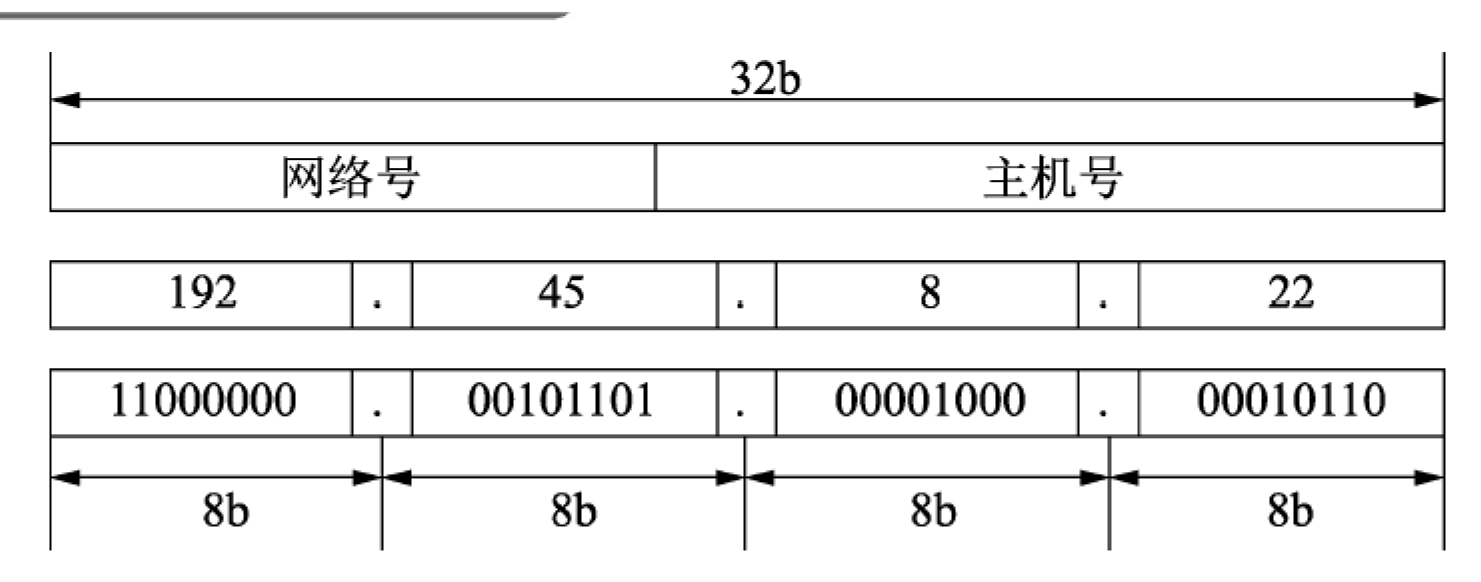



图 1-27　IP 地址的组成与表示

1. IP 地址的组成

一个 IP 地址由网络号和主机号两部分组成。同一个物理网络上的所有主机都用同一个网络号，网络上的每个主机(包括网络上的工作站、服务器和路由器等)都有一个主机号与其对应。据此把 IP 地址划分为两个部分：一部分用以标明具体的网络段，即网络号(net-id)；另一部分用以标明具体的节点，即主机号(host-id)。

2. IP 地址的表示

一个 IP 地址由 4 个字节共 32 位的数字串组成，这 4 个字节通常用小数点分隔。每个字节可用十进制数表示，如 192.45.8.22。IP 地址也可以用二进制和十六进制数表示。

3. IP 地址的分类

IP 协议的寻址方式支持 5 种不同的网络类型，即 A 类、B 类、C 类、D 类和 E 类。其中，A、B、C 类地址是基本的 Internet 地址，是用户使用的地址；D 类地址称为组播地址(多点播送地址)；而 E 类地址尚未使用，以保留将来备用。IP 地址的最左边的一个或多个二进制位通常用来指定网络的类型。例如，A 类地址的第一位为“0”，B 类地址的前两位为“10”，C 类地址的前 3 位为“110”。图 1-28 和表 1-8 说明了 5 种不同网络类型 IP 地址的特征和地址容量。

0　1　2　3　4　7 8　15 16　23 24　31

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A类地址 | 0 | 网络号 | | | | 主机号 | |
| B类地址 | 1 | 0 | 网络号 | | | 主机号 | |
| C类地址 | 1 | 1 | 0 | 网络号 | | 主机号 | |
| D类地址 | 1 | 1 | 1 | 0 | 组播地址 | | |
| E类地址 | 1 | 1 | 1 | 1 | 0 | 保留将来备用 | |

图 1-28　IP 地址的分类

表 1-8　Internet 的 IP 地址空间容量

| IP 地址类型 | 第一字节<br>十进制范围 | 二进制固定<br>最高位 | 二进制<br>网络位 | 网络数 | 二进制<br>主机位 | 主机数 |
|---|---|---|---|---|---|---|
| A 类 | 0～127 | 0 | 8 位 | 126 | 24 位 | 16 777 214 |
| B 类 | 128～191 | 10 | 16 位 | 16 384 | 16 位 | 65 534 |

续表

| IP 地址类型 | 第一字节十进制范围 | 二进制固定最高位 | 二进制网络位 | 网络数 | 二进制主机位 | 主机数 |
|---|---|---|---|---|---|---|
| C 类 | 192～223 | 110 | 24 位 | 2 097 152 | 8 位 | 254 |
| D 类 | 224～239 | 1110 | 组播地址 | | | |
| E 类 | 240～255 | 11110 | 保留将来备用 | | | |

A 类：一个 A 类 IP 地址由一个字节的网络地址和 3 个字节的主机地址组成，网络地址的最高位必须是“0”(每个字节有 8 位二进制数)。8 位作为网络号，24 位作为主机号，最多可以表示 126 个网络号(0 和 127 用作特殊地址)，每个 A 类地址主机数最多可有 $2^{24}-2$(16 777 214)个。

B 类：一个 B 类 IP 地址由两个字节的网络地址和两个字节的主机地址组成，网络地址的最高两位必须是“10”。16 位作为网络号，16 位作为主机号，最多可以表示 $2^{14}$(16 384)个网络号，每个 B 类地址主机数最多可有 $2^{16}-2$(65 534)个。

C 类：一个 C 类地址是由 3 个字节的网络地址和 1 个字节的主机地址组成，网络地址的最高 3 位必须是“110”。24 位作为网络号，8 位作为主机号。共有 $2^{21}$(2 097 152)个网络号，每个 C 类地址主机数不超过 $2^{8}-2$(254)个。

D 类：用于多点播送。第一个字节以“1110”开始。因此，任何第一个字节大于 223 小于 240 的 IP 地址是组播地址。

E 类：以“11110”开始，是保留将来备用的地址。

4. IP 地址的特殊形式

IP 地址除了可用于标识一台主机外，还有几种用于表示特殊意义的形式，如表 1-9 所示。

表 1-9　一般不使用的特殊 IP 地址

| 特殊地址 | net-id | host-id | 源地址使用 | 目的地址使用 |
|---|---|---|---|---|
| 本网络的本台主机 | 全 0 | 全 0 | 可以 | 不可以 |
| 本网络的某个主机 | 全 0 | host-id | 不可以 | 可以 |
| 网络地址 | net-id | 全 0 | 可以 | 可以 |
| 直接广播地址 | net-id | 全 1 | 不可以 | 可以 |
| 受限广播地址 | 全 1 | 全 1 | 不可以 | 可以 |
| 环回地址 | 127 | 任何数 | 可以 | 可以 |

(1) 本网络的本台主机。若一个 IP 地址全由“0”组成，即 0.0.0.0，表示在本网络上的本台主机。当一台主机在运行引导程序但又不知道其 IP 地址时使用该地址。

(2) 本网络的某个主机。网络号各位全为“0”的 IP 地址，表示在这个网络中的特定主机。它用于向同网络中其他主机发送报文。

(3) 网络地址。主机号各位全为“0”的 IP 地址，标识本网络的网络地址。

(4) 直接广播地址(有时简称为广播地址)。主机号各位全为“1”的 IP 地址。它用于将一个分组发送给特定网络上的所有主机，即对全网广播。

(5) 受限广播地址。网络号和主机号都为“1”的 IP 地址(即 255.255.255.255)。它也是对当前网络进行广播，多数是用在当一台主机在运行引导程序时，但又不知道其 IP 地址而需要向服务器获取 IP，这时用该地址作为目的地址发送分组。

(6) 环回地址(Loopback Address)。A 类网络地址 127.x.x.x 是一个保留地址，用于网络软件测试以及本地进程间的通信。

5. 保留 IP 地址

如果一个组织不需要接入到互联网上，但需要在其网络上运行 TCP/IP 协议，最佳选择是使用保留地址。保留地址不需要从互联网管理机构申请，任何组织都可以使用这些地址。这些地址在一个组织内部是唯一的，但从全局来看却不是唯一的。同时互联网的路由器也不转发目标地址为保留地址的数据包。保留地址如表 1-10 所示。

表 1-10 Internet 的保留 IP 地址空间

| 类　型 | 网 络 号 | 网 络 数 |
| --- | --- | --- |
| A 类 | 10.0.0.0 | 1 |
| B 类 | 172.16.0.0～172.31.0.0 | 16 |
| C 类 | 192.168.0.0～192.168.255.0 | 256 |

### 1.6.1.2 子网的划分

1. 划分子网的必要性

(1) IP 地址空间利用率很低。由于 Internet 的 IP 地址采用两级结构，即网络号和主机号，这样的设计有不够合理的地方。IP 地址中的 A～C 类地址，可供分配的网络号码超过 211 万个，而这些网络上的主机号的总数则超过 37.2 亿个，初看起来，似乎 IP 地址足够全世界来使用(在 20 世纪 70 年代初期设计 IP 地址时就是这样认为的)。其实不然。第一，当初没有预计到计算机会普及得如此之快，各种局域网以及局域网上的主机数目急剧增长。第二，IP 地址在使用时有很大的浪费。例如，某个单位申请到了一个 B 类地址，但该单位只有 1 万台主机。于是，在一个 B 类地址中的其余 55 000 多个主机号就白白浪费了，因为其他单位的主机无法使用这些号码。

(2) 大型的网络将影响网络性能。从网络吞吐量考虑，将大量主机安装在一个网络上往往会影响网络的性能。当网络上工作的主机数小于一定数值时，网络的吞吐量和网络上工作的主机数大约成正比。但是当网络上工作的主机数超过一定数量时，拥塞就可能产生，这就导致网络的吞吐量增加、速度变慢，网络性能甚至会随着主机数的增加而下降。

(3) IP 地址的两级结构不够灵活。有时情况紧急，一个单位需要在新的地点马上开通一个新网络。但是在申请到一个新的 IP 地址之前，新增加的网络不可能连接到互联网上工作。用户希望有一种方法，使本单位能随时灵活地增加网络，而不必事先到互联网管理机构去申请新的网络号，但原来的两级 IP 地址结构无法做到这一点。

2. 从两级 IP 地址到三级 IP 地址

为了解决上述问题，在 IP 地址中又增加了一个“子网号字段”，使原来两级的 IP 地址变成为三级的 IP 地址，这样就能够较好地解决上述问题，并且使用起来也很灵活。划分子

网的基本思路如下。

(1) 一个拥有许多物理网络的单位，可将其物理网络划分为若干个子网(Subnet)。划分子网纯属一个单位内部的事情，本单位以外的网络看不见这个网络由多少子网组成，对外仍表现为一个没有划分子网的网络。

(2) 划分子网的方法是从 IP 地址的主机号借用若干位作为子网号 subnet-id，而主机号 host-id 也就相应地减少了若干位。于是，两级的 IP 地址在本单位内部就变为三级 IP 地址，即网络号 net-id、子网号 subnet-id 和主机号 host-id，如图 1-29 所示。

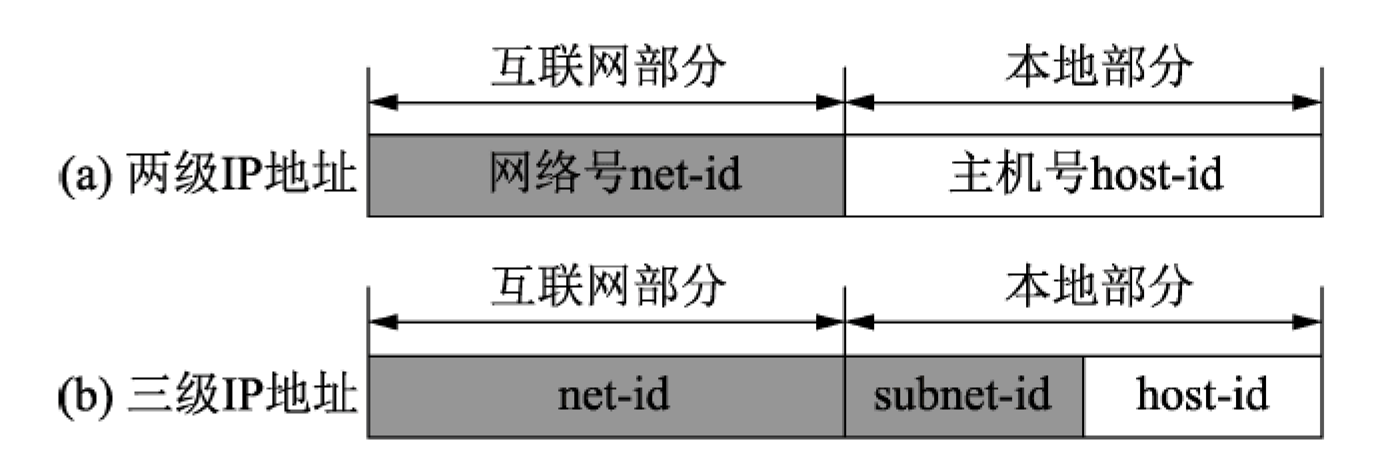



图 1-29　从两级 IP 地址到三级 IP 地址(一)

(3) 凡是从其他网络发送给本单位某个主机的 IP 数据报，仍然是根据 IP 数据报的目的网络号 net-id 找到连接在本单位网络上的路由器。但此路由器在收到 IP 数据报后，再按目的网络号 net-id 和子网号 subnet-id 找到目的子网，并将 IP 数据报交付给目的主机。

下面用一个例子来说明划分子网的概念。一个单位拥有一个 B 类 IP 地址，网络地址是 141.14.0.0(net-id 是 141.14)。凡目的地址为 141.14.x.x 的数据报都被送到这个网络上的路由器 R1。

现将图 1-30 所示的网络划分为 3 个子网，如图 1-31 所示。这里假设子网号 subnet-id 占 8 位，因此在增加子网号后主机号 host-id 就只有 8 位。所划分的 3 个子网分别是 141.14.2.0、141.14.7.0 和 141.14.99.0。在划分子网后，整个网络对外仍表现为一个网络，其网络地址仍然是 141.14.0.0。但路由器 R1 收到数据报后，再根据数据报的目的地址将其转发到相应的子网。

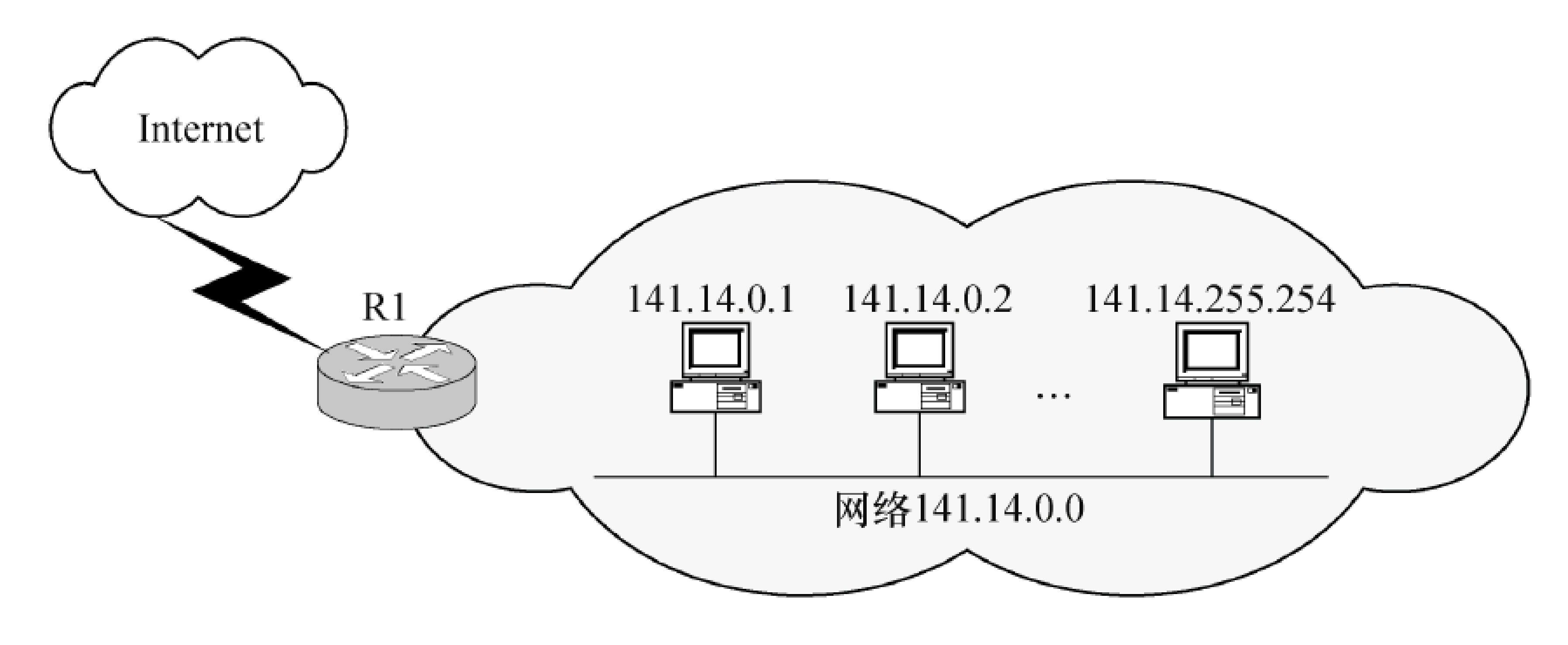



图 1-30　从两级 IP 地址到三级 IP 地址(二)

### 3. 子网掩码

虽然上面已经把一个网络划分为若干个子网，但路由器 R1 必须知道数据报中目的 IP 地址的网络号 net-id、子网号 subnet-id 和主机号 host-id 各是多少位，这就需要通过子网掩码(Subnet Mask)来实现。

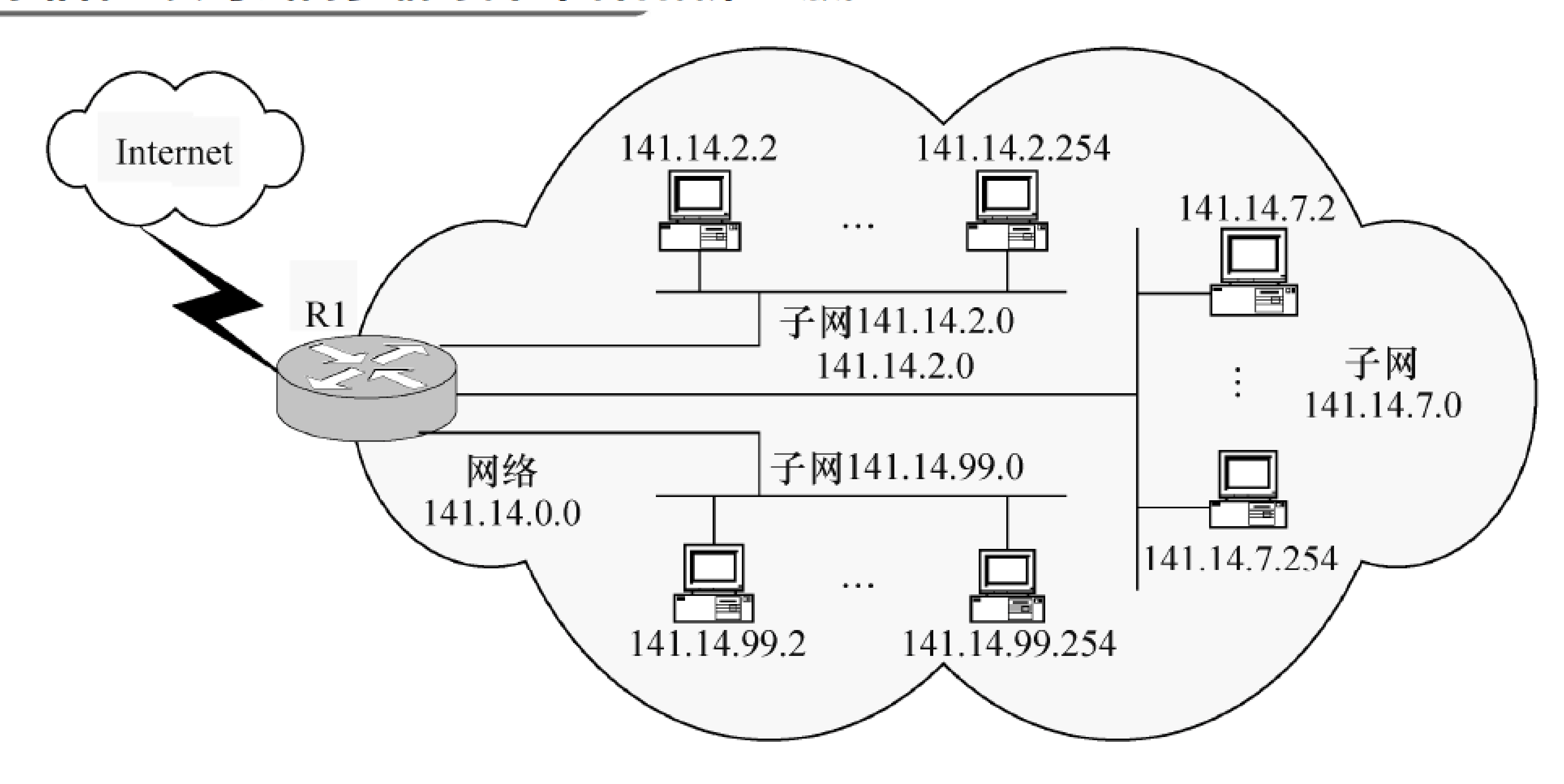



图 1-31　从两级 IP 地址到三级 IP 地址(三)

子网掩码和 IP 地址一样，也是 32 位长，由一串 1 和跟随的一串 0 组成。子网掩码中的 1 对应于 IP 地址中的网络号 net-id 和子网号 subnet-id，而子网掩码中的 0 对应于 IP 地址中的主机号 host-id。要得到网络或子网地址，只需将 IP 地址和子网掩码进行按位“与”(AND)运算即可。图 1-32 说明了子网掩码的工作方式。

| | | |
|---|---|---|
| IP地址 | 141.14.2.21 | 10001101　00001110　00000010　00010101 |
| 子网掩码 | 255.255.0.0 | 11111111　11111111　00000000　00000000 |
| 网络地址 | 141.14.0.0 | 10001101　00001110　00000000　00000000 |

(a) 不划分子网

| | | |
|---|---|---|
| IP地址 | 141.14.2.21 | 10001101　00001110　00000010　00010101 |
| 子网掩码 | 255.255.255.0 | 11111111　11111111　11111111　00000000 |
| 网络地址 | 141.14.2.0 | 10001101　00001110　00000010　00000000 |

(b) 划分子网

图 1-32　进行按位“与”(AND)运算可得到网络地址

图 1-32(a)表示在未划分子网情况下，网络地址是 IP 地址与它默认的子网掩码(255.255.0.0)按位“与”运算的结果，即将主机号 host-id 设置为 0 的 IP 地址。图 1-32(b)表示在划分子网情况下，当主机号借用 8 位作为子网号 subnet-id，子网掩码中“1”的个数相应地增加 8，即 255.255.255.0。这时将子网掩码和 IP 地址按位“与”运算就得到了子网地址。这里要注意是：网络地址(在划分子网时常称为子网地址)并不仅仅是一个子网号 subnet-id，而是将主机号 host-id 设置为 0 的 IP 地址。可以看出，子网掩码不能单独存在，它必须结合 IP 地址一起使用。

与 IP 地址相同，子网掩码通常也使用点分十进制表示法表示，如 255.255.255.0、255.255.255.240 等。有时为了表示方便，通常在 IP 地址后加一个“/网络号和子网号位数”。例如，210.45.12.58/28 就表示该 IP 地址的网络号 net-id 和子网号 subnet-id 共占用 28 位，主机号占用 32−28=4 位，如果用点分十进制表示法表示，则子网掩码是 255.255.255.240 (11111111.11111111.11111111.11110000)。

使用子网掩码的好处是：不管网络是否划分子网，也不管 IP 地址中的网络号 net-id 和子网号 subnet-id 是多少位，只要将子网掩码和 IP 地址进行按位“与”运算，就可立即得出网络地址。这样在路由器处理到来的 IP 分组时就可采用同样的算法。

如果一个网络不划分子网，那么该网络的子网掩码就使用默认子网掩码。默认子网掩码中值为 1 的位与 IP 地址的网络号 net-id 所占位正好相对应。因此默认子网掩码和不划分子网的 IP 地址按位“与”(AND)运算，就得出该 IP 地址的网络地址，这样做可以不用查找该地址的分类位就能知道这是哪一类的 IP 地址。显然，A 类、B 类和 C 类网络默认子网掩码分别是 255.0.0.0(/8)、255.255.0.0(/16)、255.255.255.0(/24)，如图 1-33 所示。

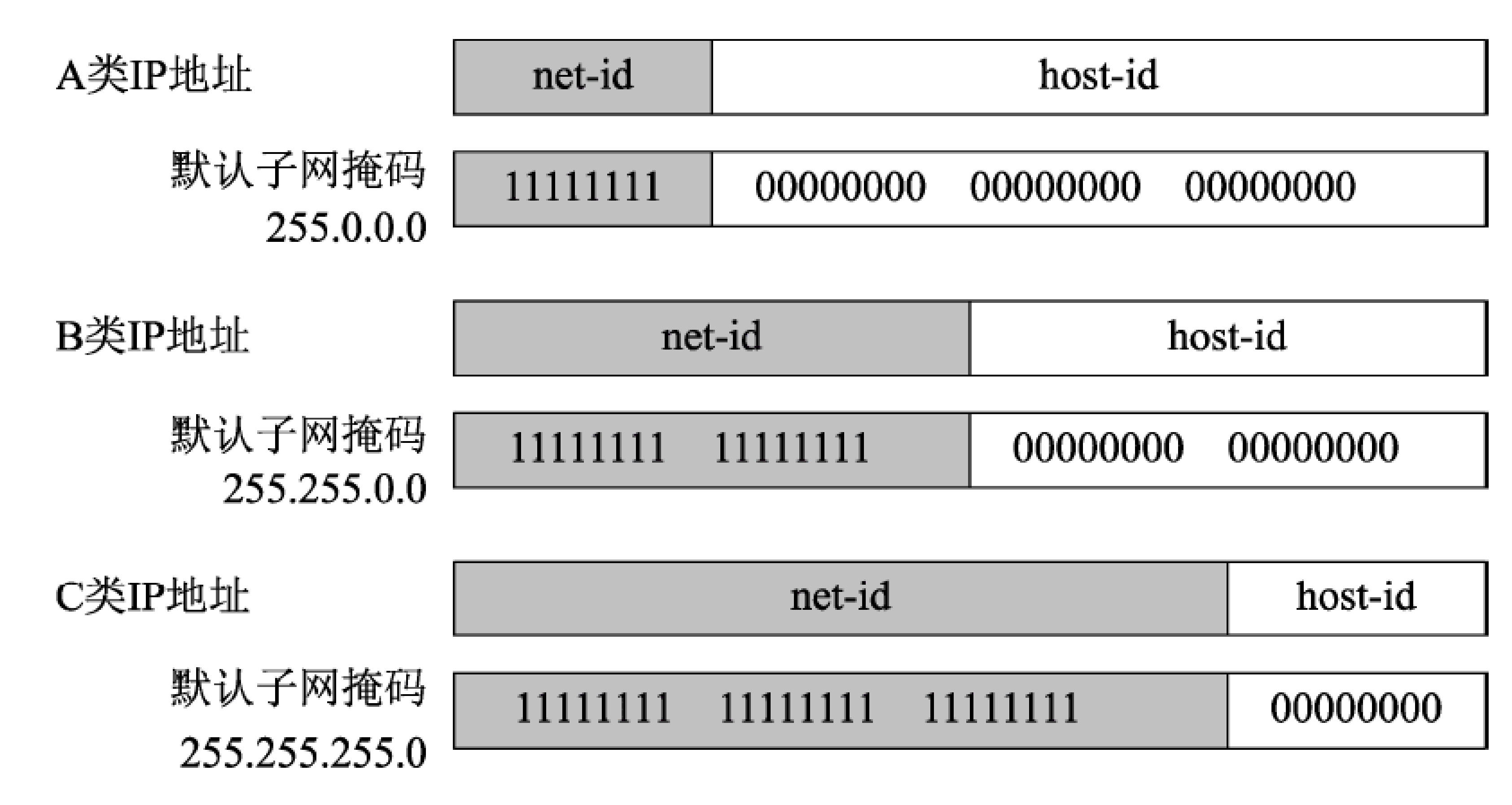



图 1-33　A 类、B 类和 C 类 IP 地址的默认子网掩码

4. 划分子网示例

1) B 类地址的子网规划示例

B 类地址由两个字节的网络号 net-id 和两个字节的主机号 host-id 组成。一个得到 B 类地址的组织可以有一个单独的物理网络，在此网络上连接的计算机可达 65 534($2^{16}-2$)个。但是，若该组织愿意有更多的物理网络，则这个大的范围可划分成许多更小的范围。表 1-11 说明了一个 B 类地址可以有多少种子网划分的方法。在采用固定长度子网时划分的所有子网的子网掩码都是相同的。

表 1-11　B 类地址的子网划分选择(使用固定长度子网)

| 子网位数 | 子网掩码 | 子 网 数 | 主 机 数 |
|---|---|---|---|
| 2 | 255.255.192.0 | 2 | 16 382 |
| 3 | 255.255.224.0 | 6 | 8190 |
| 4 | 255.255.240.0 | 14 | 4094 |
| 5 | 255.255.248.0 | 30 | 2046 |

续表

| 子网位数 | 子网掩码 | 子 网 数 | 主 机 数 |
|---|---|---|---|
| 6 | 255.255.252.0 | 62 | 1022 |
| 7 | 255.255.254.0 | 126 | 510 |
| 8 | 255.255.255.0 | 254 | 254 |
| 9 | 255.255.255.128 | 510 | 126 |
| 10 | 255.255.255.192 | 1022 | 62 |
| 11 | 255.255.255.224 | 2046 | 30 |
| 12 | 255.255.255.240 | 4094 | 14 |
| 13 | 255.255.255.248 | 8190 | 6 |
| 14 | 255.255.255.252 | 16 382 | 2 |

例如，一个具有B类地址的组织的网络号为*X*.*Y*.0.0(128≤*X*≤191)，需要至少12个子网，试找出子网掩码和每个子网的配置。因为需要至少12个子网，因此至少需要向主机号host-id借4位($2^3-2\leqslant12\leqslant2^4-2$)来构造子网，网络号net-id和子网号subnet-id共12位(8+4=12)，所以子网掩码为11111111.11111111.11110000.00000000，即255.255.240.0。每个子网有4096($2^{12}$=4096)个地址，其中第一个地址用来定义子网(子网地址)，而最后一个地址用于子网内广播(广播地址)，这就表明连接到每一个子网上的计算机数最多是4094。表1-12列出了每个子网的地址范围。

表1-12 B类地址的子网划分示例(使用固定长度子网)

| 子 网 | 子网地址 | 地址范围 | 广播地址 | 说 明 |
|---|---|---|---|---|
| 第0个子网 | *X*.*Y*.0.0 | *X*.*Y*.0.1～*X*.*Y*.15.254 | *X*.*Y*.15.255 | 保留，不可用 |
| 第1个子网 | *X*.*Y*.16.0 | *X*.*Y*.16.1～*X*.*Y*.31.254 | *X*.*Y*.31.255 | 可用 |
| 第2个子网 | *X*.*Y*.32.0 | *X*.*Y*.32.0～*X*.*Y*.47.254 | *X*.*Y*.47.255 | 可用 |
| ⋮ | ⋮ | ⋮ | ⋮ | 可用 |
| 第14个子网 | *X*.*Y*.224.0 | *X*.*Y*.224.0～*X*.*Y*.239.254 | *X*.*Y*.239.255 | 可用 |
| 第15个子网 | *X*.*Y*.240.0 | *X*.*Y*.240.1～*X*.*Y*.255.254 | *X*.*Y*.255.255 | 保留，不可用 |

**注意：** 根据RFC 950的规定，进行子网划分时对于子网号subnet-id为全0和全1的子网不允许使用，因此表1-12中第0个子网和第15个子网是不可用的。但随着无分类域间路由选择CIDR的广泛使用，现在全0和全1的子网也可以使用，但一定要谨慎使用，要弄清所使用的路由器是否支持全0和全1的子网。

2) C类地址的子网规划示例

C类地址由3个字节的网络号net-id和一个字节的主机号host-id组成。一个得到C类地址的组织可以有一个单独的物理网络，在此网络上连接的计算机可达254($2^8-2$)个。但是，若该组织愿意有更多的物理网络，则这个大的范围可划分成许多更小的范围。表1-13说明了一个C类地址可以有多少种子网划分的方法(在采用固定长度子网时，划分的所有子网的子网掩码都是相同的)。

表 1-13　C 类地址的子网划分选择(使用固定长度子网)

| 子网位数 | 子网掩码 | 子 网 数 | 主 机 数 |
|---|---|---|---|
| 2 | 255.255.255.192 | 2 | 62 |
| 3 | 255.255.255.224 | 6 | 30 |
| 4 | 255.255.255.240 | 14 | 14 |
| 5 | 255.255.255.248 | 30 | 6 |
| 6 | 255.255.255.252 | 62 | 2 |

例如，一个具有 C 类地址的组织的网络号为 *X.Y.Z.*0(192≤*X*≤223)，需要至少 5 个子网，试找出子网掩码和每个子网的配置。因为需要至少 5 个子网，划分时至少要 7 个子网，5 个是可用的，两个保留为特殊地址，不可用，因此至少需要向主机号 host-id 借 3 位($2^2-2≤5≤2^3-2$)来构造子网，网络号 net-id 和子网号 subnet-id 共 27(24+3)位，所以子网掩码为 11111111.11111111.11111111.11100000，即 255.255.255.224。每个子网有 32 个($2^5=32$)地址，其中第一个地址用来定义子网(子网地址)，而最后一个地址用于子网内广播(广播地址)，这就表明连接到每一个子网上的计算机数最多是 30。表 1-14 列出了每个子网的地址范围。

表 1-14　C 类地址的子网划分实例(使用固定长度子网)

| 子　网 | 子网地址 | 地址范围 | 广播地址 | 说　明 |
|---|---|---|---|---|
| 第 0 个子网 | *X.Y.Z.*0 | *X.Y.Z.*1～*X.Y.Z.*30 | *X.Y.Z.*31 | 保留，不可用 |
| 第 1 个子网 | *X.Y.Z.*32 | *X.Y.Z.*33～*X.Y.Z.*62 | *X.Y.Z.*63 | 可用 |
| 第 2 个子网 | *X.Y.Z.*64 | *X.Y.Z.*65～*X.Y.Z.*94 | *X.Y.Z.*95 | 可用 |
| ⋮ | ⋮ | ⋮ | ⋮ | 可用 |
| 第 6 个子网 | *X.Y.Z.*192 | *X.Y.Z.*193～*X.Y.Z.*222 | *X.Y.Z.*223 | 可用 |
| 第 7 个子网 | *X.Y.Z.*224 | *X.Y.Z.*225～*X.Y.Z.*254 | *X.Y.Z.*255 | 保留，不可用 |

A 类地址的子网规划方法与 B 类、C 类相似，因篇幅所限，这里不作详细介绍。

5. 可变长子网掩码(VLSM)

互联网允许一个地点使用变长子网划分。下面举例说明什么时候有这种需要。例如，一个具有 C 类地址的地点需要划分为 5 个子网，其连接的主机数分别为 60、60、60、30 和 30。这个地点不能使用给子网分配两个位的掩码，因为这样将只有 4 个可连接 62(256/4−2=62)台主机的子网。在这个地点使用给子网分配 3 个位的掩码也不行，因为这样将有 8 个可连接 30(256/8−2=30)台主机的子网(应注意，这里放松了对特殊地址的要求，即子网号为全 0 和全 1 可用)。

解决这个问题的一种方法是使用变长子网划分，在这种配置中路由器使用两个不同的掩码。它先使用具有 26 个 1 的掩码(11111111.11111111.11111111.11000000 或 255.255.255.192)，将网络划分为 4 个子网。然后再对其中的一个子网使用具有 27 个 1 的掩码(11111111.11111111.11111111.11100000 或 255.255.255.224)，将其划分为两个更小的子网(见图 1-34)。

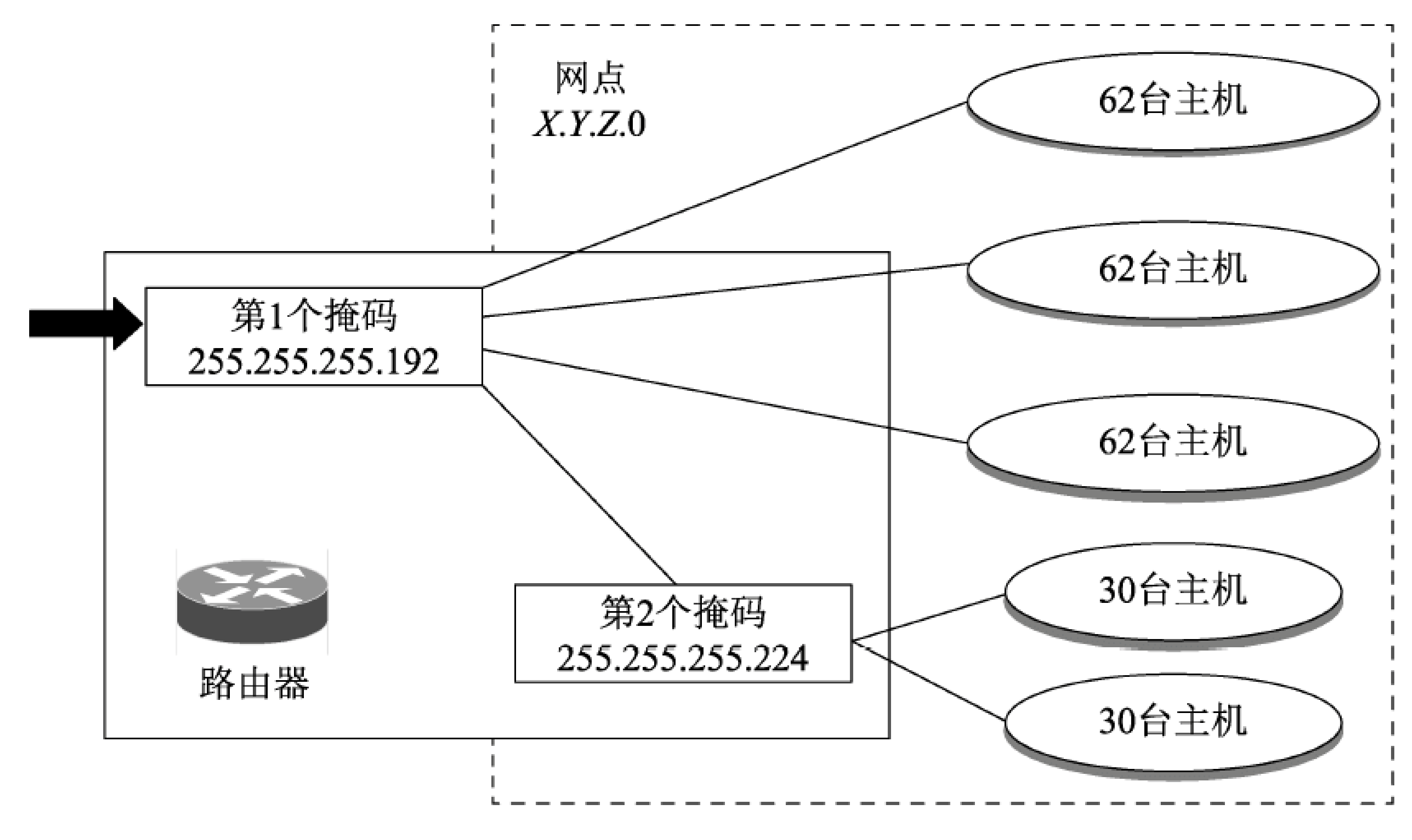



图 1-34　可变长子网划分

### 1.6.1.3　超网和无分类编址

虽然 A 类和 B 类地址几乎用完了，但 C 类地址目前还能申请到。然而 C 类地址空间只能容纳最多 254 台主机，这可能无法满足一个组织的需要，甚至一个中等规模的组织也会需要更多的地址。

一种解决问题的方法是构成超网(Supernet)。为此，一个组织可申请一块而不是只申请一个 C 类地址。例如，一个需要 1000 个地址的组织可申请 4 个 C 类地址。这个组织就可以在一个超网中、在 4 个网络中或在超过 4 个子网中使用这些地址。在图 1-35 中，4 个 C 类地址合并为一个超网。

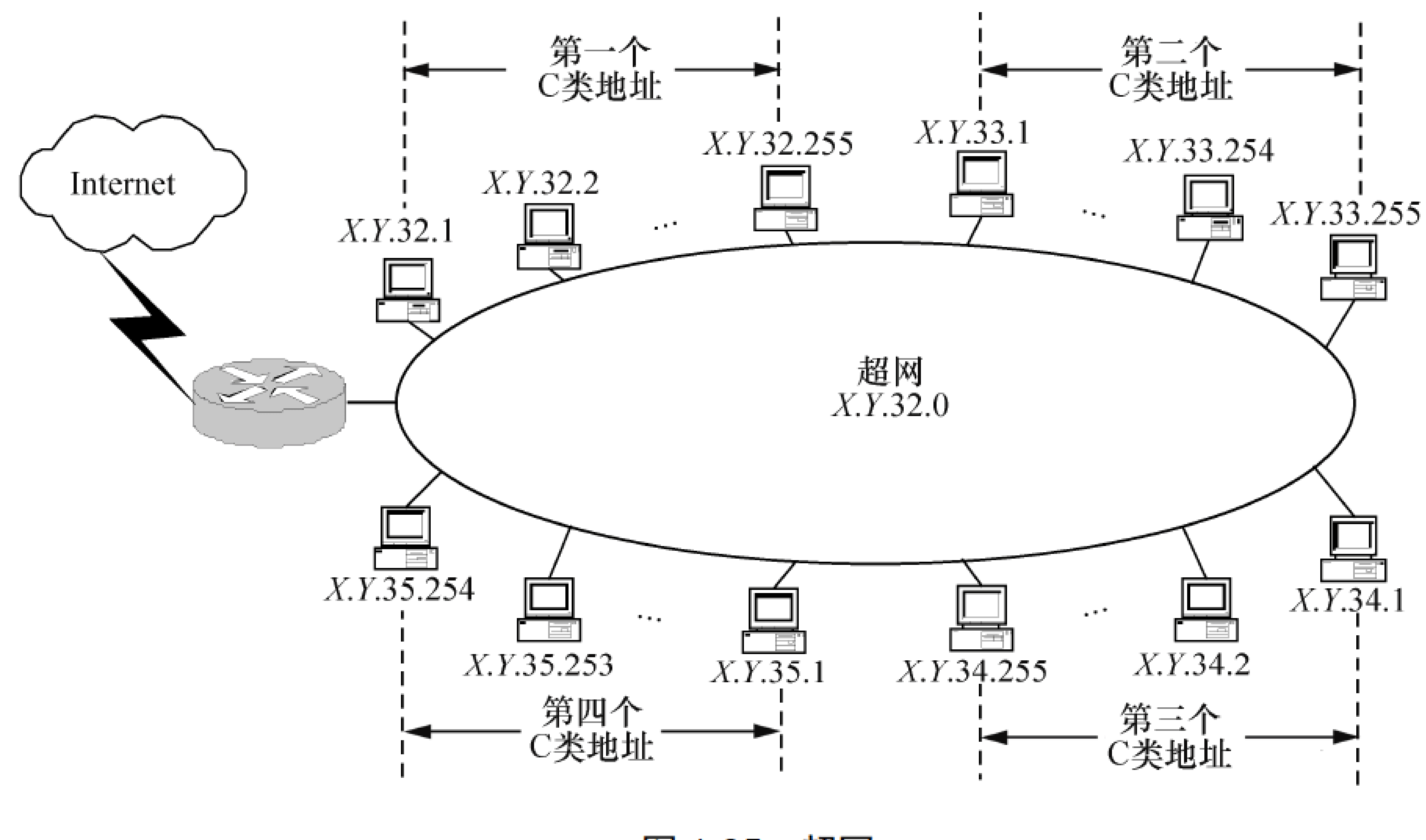



图 1-35　超网

若要给超网掩码指派一块 C 类网络地址，只要地址数是 2 的整数次方(2，4，8，16，…)即可。C 类地址的默认掩码是 255.255.255.0，即 24 个 1 后面跟上 8 个 0。如果将其中的某些 1 改变为 0，就可得到一组 C 类地址的超网掩码。超网掩码与子网掩码中的一些做法相

反。在子网掩码中，将默认掩码中的 host-id 部分的某些 0 改变为 1。在超网掩码中，将 net-id 部分中的某些 1 改变为 0。要注意到，在超网掩码中全 1 的位置定义了最低地址。例如，图 1-36 所示的超网掩码，开始地址可以是 *X.Y.*32.0，但不能是 *X.Y.*33.0。将最低地址与超网掩码组合起来就能唯一地定义属于一个超网的地址范围，另一个定义地址范围的方法是使用最低地址和在此范围内的地址数来定义。

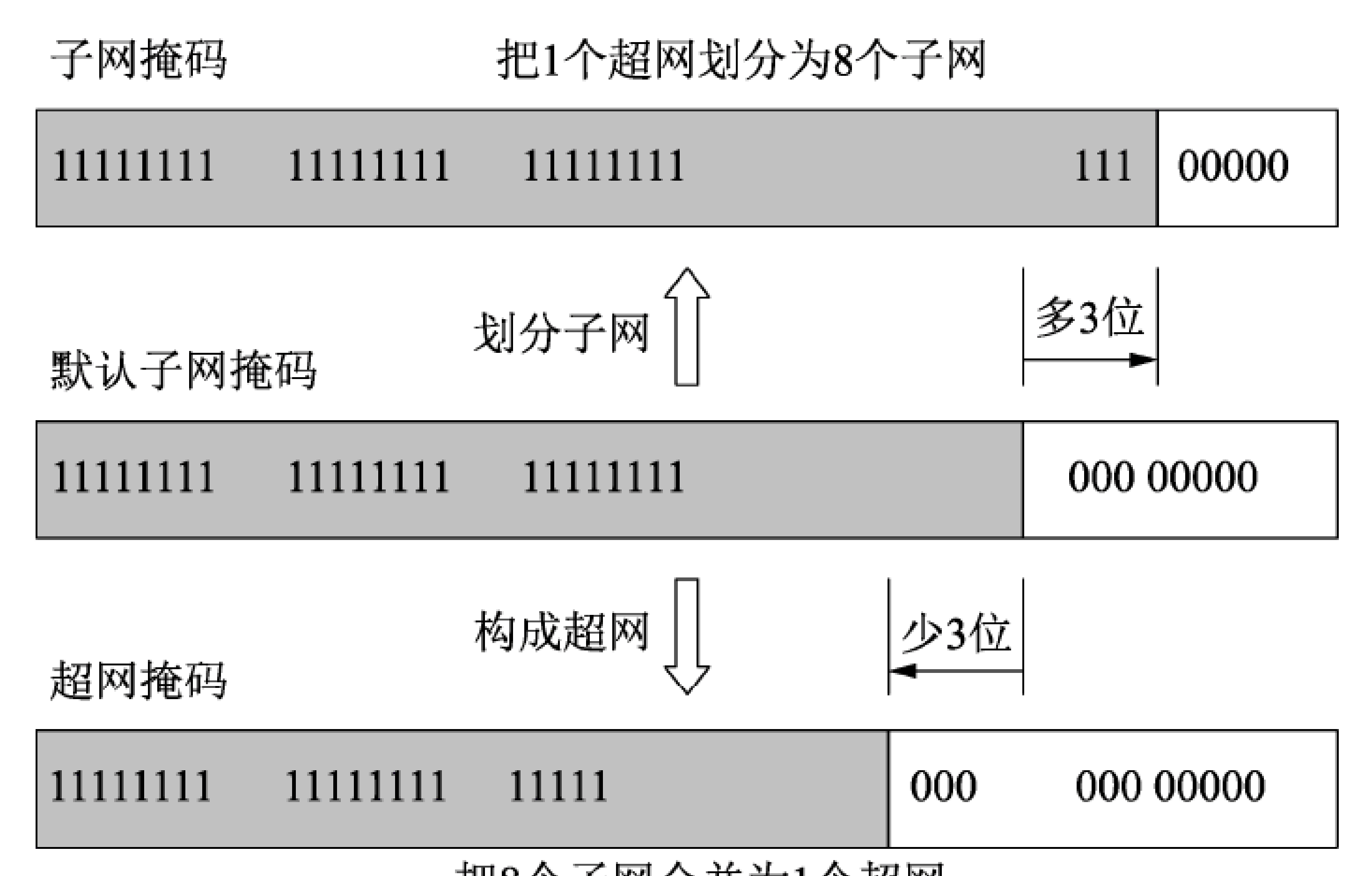



图 1-36　超网掩码

例如，用超网掩码 255.255.252.0 可以将 4 个 C 类地址合并为一个超网。如果选择的第一个地址是 *X.Y.*32.0，则其他 3 个地址就是 *X.Y.*33.0、*X.Y.*34.0 和 *X.Y.*35.0。当路由器收到一个分组时，就将超网掩码与目的地址作按位“与”(AND)运算，并将结果与最低地址相比较。若结果与最低地址一致，则该分组就属于这个超网。

假定一个分组到达目的地址 *X.Y.*33.4。在同掩码 255.255.252.0 作按位“与”(AND)运算后，结果为 *X.Y.*32.0，它与最低地址一致，因此该分组属于这个超网。

现在假定目的地址为 *X.Y.*39.12 的分组到达，在同掩码 255.255.252.0 作按位“与”(AND)运算后，结果为 *X.Y.*36.0，它与最低地址不一致，因此该分组不属于这个超网。

在 VLSM 的基础上又进一步研究出无分类编址方法，它的正式名称是无分类域间路由选择(Classless Inter-Domain Routing，CIDR)。CIDR 最主要的特点有以下两个。

(1)  CIDR 消除了传统 A 类、B 类和 C 类地址以及划分子网的概念，从而更加有效地分配 IPv4 的地址空间。CIDR 使用各种长度的“网络前缀”(Network-Prefix)来代替分类地址中的网络号和子网号，而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀，使 IP 地址从三级编址(使用子网掩码)又回到两级编址，但这是一个无分类的两级编址。CIDR 使用“斜线记法”，它又称为 CIDR 记法，即在 IP 地址后面加上一个斜线“/”，然后写上网络前缀所占的位数(这个数值对应于三级编址中子网掩码中位 1 的个数)。例如，128.14.146.158/20 表示在这 32 位中，前 20 位表示网络前缀，而后面 12 位为主机号。

(2)  CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块是由地址块的起始地址(地址块中数值最小的一个)和地址块中的地址数来定义的。CIDR 地址块也可用斜线记法来表示。例如，128.14.32.0/20 表示的地址块共有 $2^{12}$ 个地址，而这个

地址的起始地址是 128.14.32.0。

## 1.6.2 典型例题分析

**例 1** 阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题二)

**【说明】**

某单位网络拓扑结构如图 1-37 所示，FTP 服务器的域名为 xhfip.SoftwareExam.com。

**【问题 1】**

在该单位综合布线时，连接楼 A 与楼 B 的布线子系统为 (1) ；楼 A 内网管中心服务器群至核心交换机的布线子系统为 (2) 。

(1)、(2)备选答案：

A. 水平子系统　　B. 垂直子系统　　C. 设备间子系统

D. 建筑群子系统　　E. 干线子系统　　F. 管理子系统

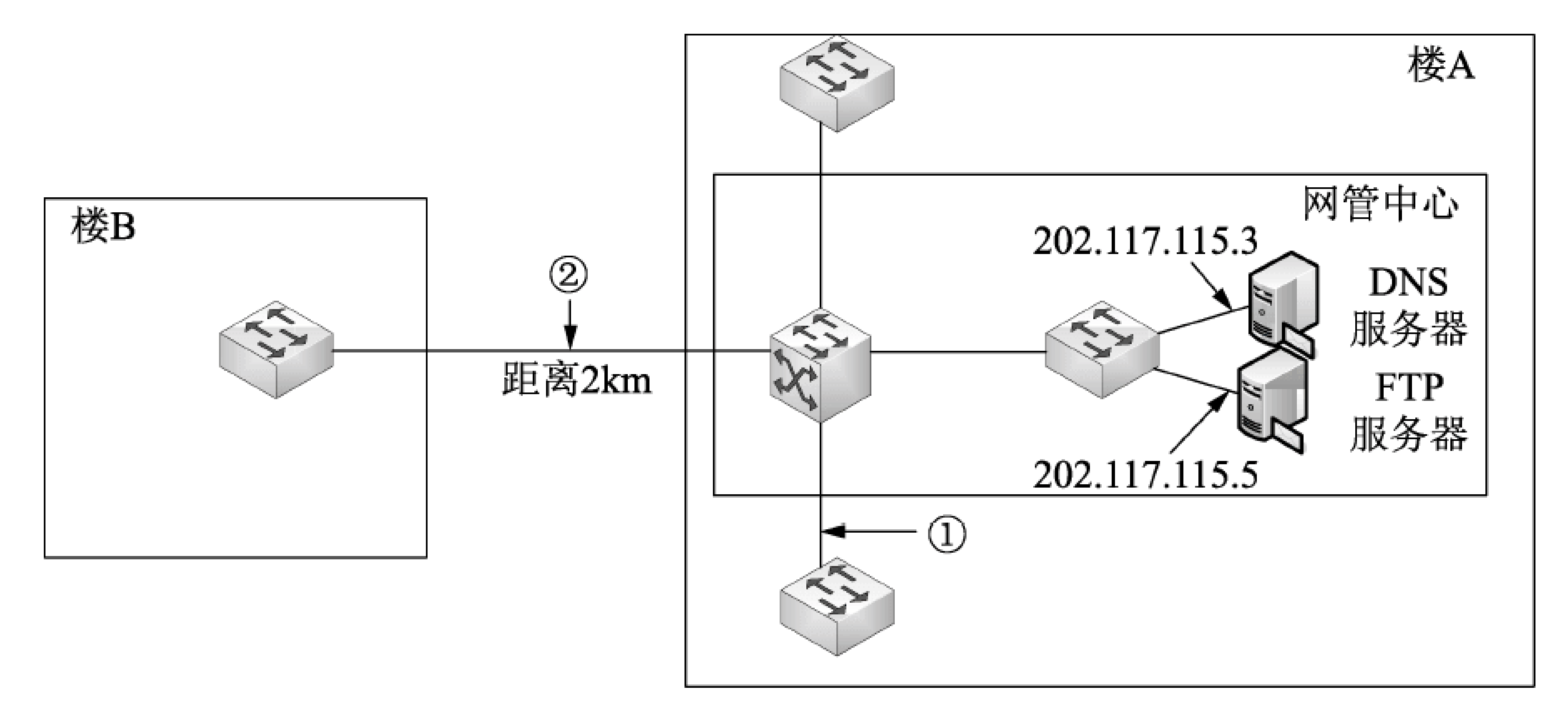



图 1-37 某单位网络拓扑结构

**【问题 2】**

图 1-38 中①的传输介质为 (3) 、②的传输介质为 (4) 。

(3)、(4)备选答案(限选一次)：

A. 单模光纤　　B. 多模光纤

**【问题 3】**(每空 1 分，共 3 分)

依据图 1-39 配置好 FTP 服务器后，其数据端口为 (5) 若尚未配置域名记录，在浏览器中可输入 URL (6) 来访问 FTP 站点。

**【问题 4】**(每空 2 分，共 4 分)

图 1-39 所示为用户组的权限设置，网站的创建者对 FTP 根目录的默认权限为 (7) 。

**【问题 5】**(2 分)

在 DNS 服务器中为 FTP 服务器配置域名记录时，新建主机如图 1-37 所示。

在图 1-40 所示的对话框中，添加的主机“名称”为 (8) ，“IP 地址”是 (9) 。如果要实现 FTP 服务器的 IP 地址和域名互查，该如何操作？

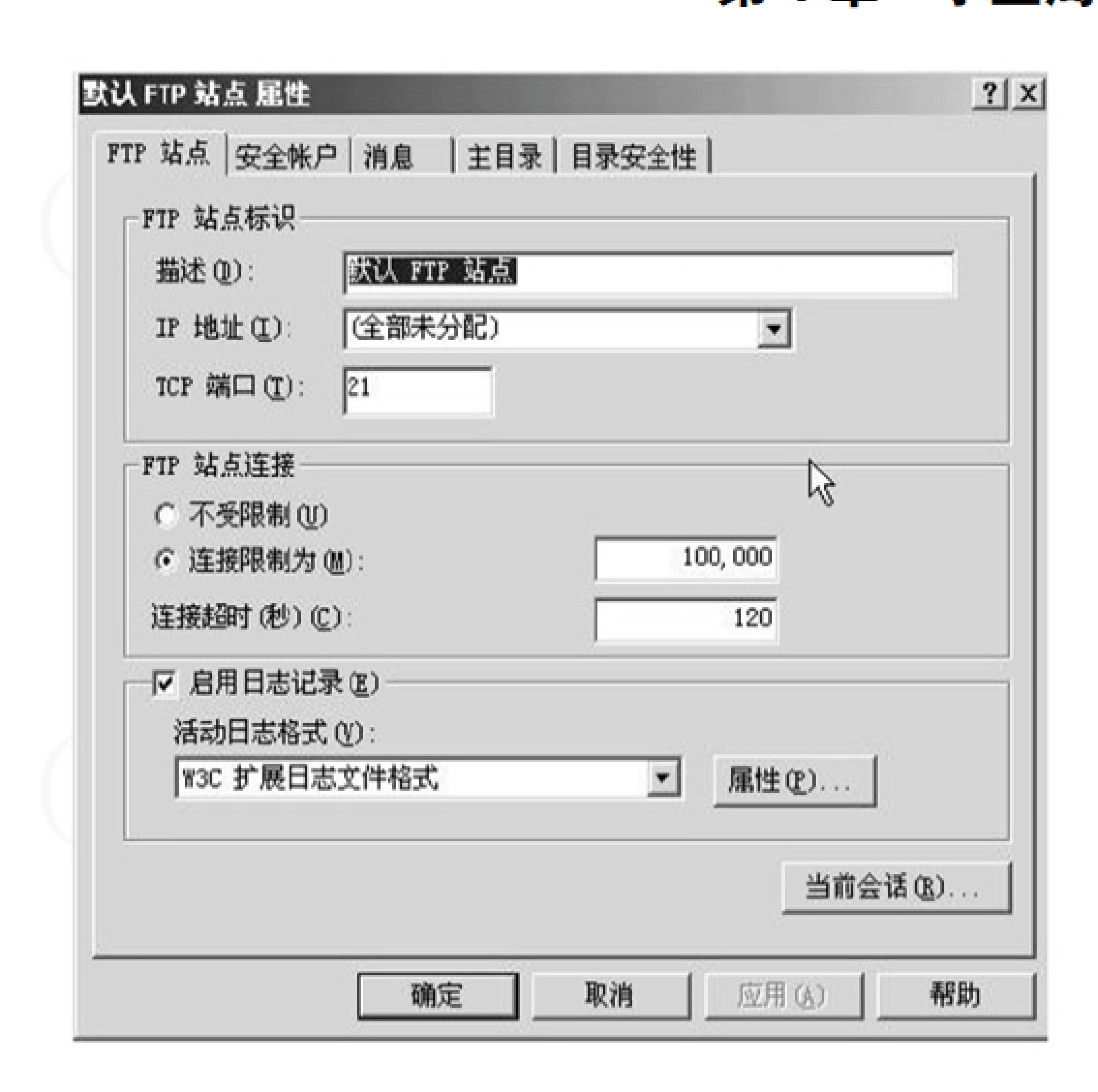



图 1-38　FTP 服务器配置图

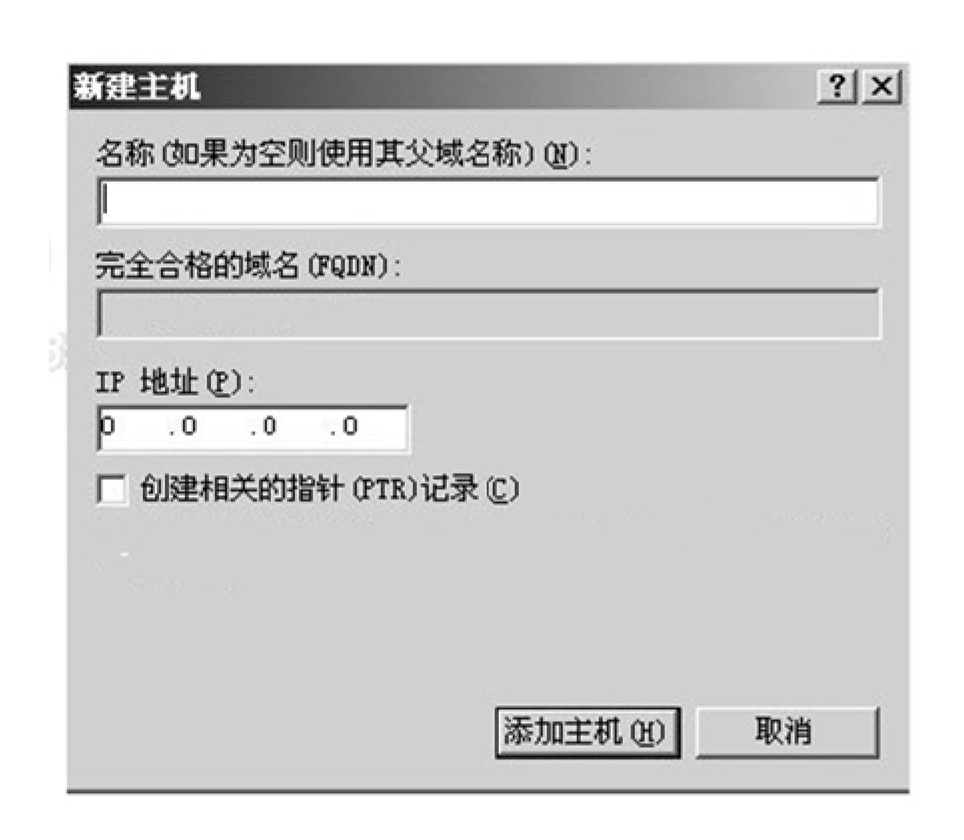



图 1-39　FTP 配置新建主机

**分析：**本试题考查综合布线、用户权限以及服务器配置相关知识，属传统考查项目。

**【问题 1】**

综合布线系统由 6 个子系统组成，即建筑群子系统、设备间子系统、干线子系统、 管理子系统、配线子系统、工作区子系统。大型布线系统需要用铜介质和光纤介质部件将 6 个子系统集成在一起。

(1) 水平子系统(Horizontal Subsystem)：由信息插座、配线电缆或光纤、配线设备和跳线等组成。国内称之为配线子系统。

(2) 垂直子系统(Backbone Subsystem)：由配线设备、干线电缆或光纤、跳线等组成。国内称之为干线子系统。

(3) 工作区子系统(WorkArea Subsystem)：为需要设置终端设备的独立区域。

(4) 管理子系统(Administration Subsystem)：针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

(5) 设备间子系统(Equipment Room Subsystem)：安装各种设备的场所，对综合布线而言，还包括安装的配线设备。

(6) 建筑群子系统(Campus Subsystem)：由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

由此，题目中连接楼 A 与楼 B 的布线子系统为建筑群子系统；楼 A 内网管中心服务器群至核心交换机的布线子系统为设备间子系统。

**【问题 2】**

图 1-37 中①处传输介质连接两个楼层，可选多模光纤，②处连接两个建筑物且距离 2km，故传输介质为单模光纤。

**【问题 3】**

默认情况下，FTP 服务器数据端口和控制端口分别是 20 和 21，控制端口也可手工设置(通常为大于 1024 的高端)，若设置好控制端口，数据端口通常为控制端口−1，图 1-39 中为 FTP 服务器设置 TCP 端口为 21，故其数据端口为 20。

在没有配置域名记录的情况下，要访问该 FTP 服务器，在浏览器中可输入 URL ftp://202.117.115.5:2121 来访问 FTP 站点。

**【问题 4】**

网站的创建者需要完全控制网站，故其对 FTP 根目录的默认权限为完全控制。

**【问题 5】**

在 DNS 服务器中为 FTP 服务器配置域名记录时，由于 FTP 服务器的域名为 xhftp.SoftwareExam.com，故添加的主机“名称”为 xhftp，“IP 地址”是 202.117.115.5。

如果要实现 FTP 服务器的 IP 地址和域名互查，即 FTP 服务器除了正向解析外还需再反向解析的功能，在图 1-40 中选中“创建相关的指针(PTR)记录(C)”复选框可实现反向解析。

答案：

**【问题 1】**

(1) D　　(2) C

**【问题 2】**

(3) B　　(4) A

**【问题 3】**

(5) 21

(6) ftp://202.117.115.5:2121

**【问题 4】**

(7) 完全控制

**【问题 5】**

(8) xhfip　　(9) 202.117.115.5　　(10) 选中“创建相关的指针(PTR)记录”复选框

**例 2**　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题一)

**【说明】**

某公司局域网拓扑图如图 1-40 所示，其中 S1 为三层交换机，S2 和 S3 为二层交换机。

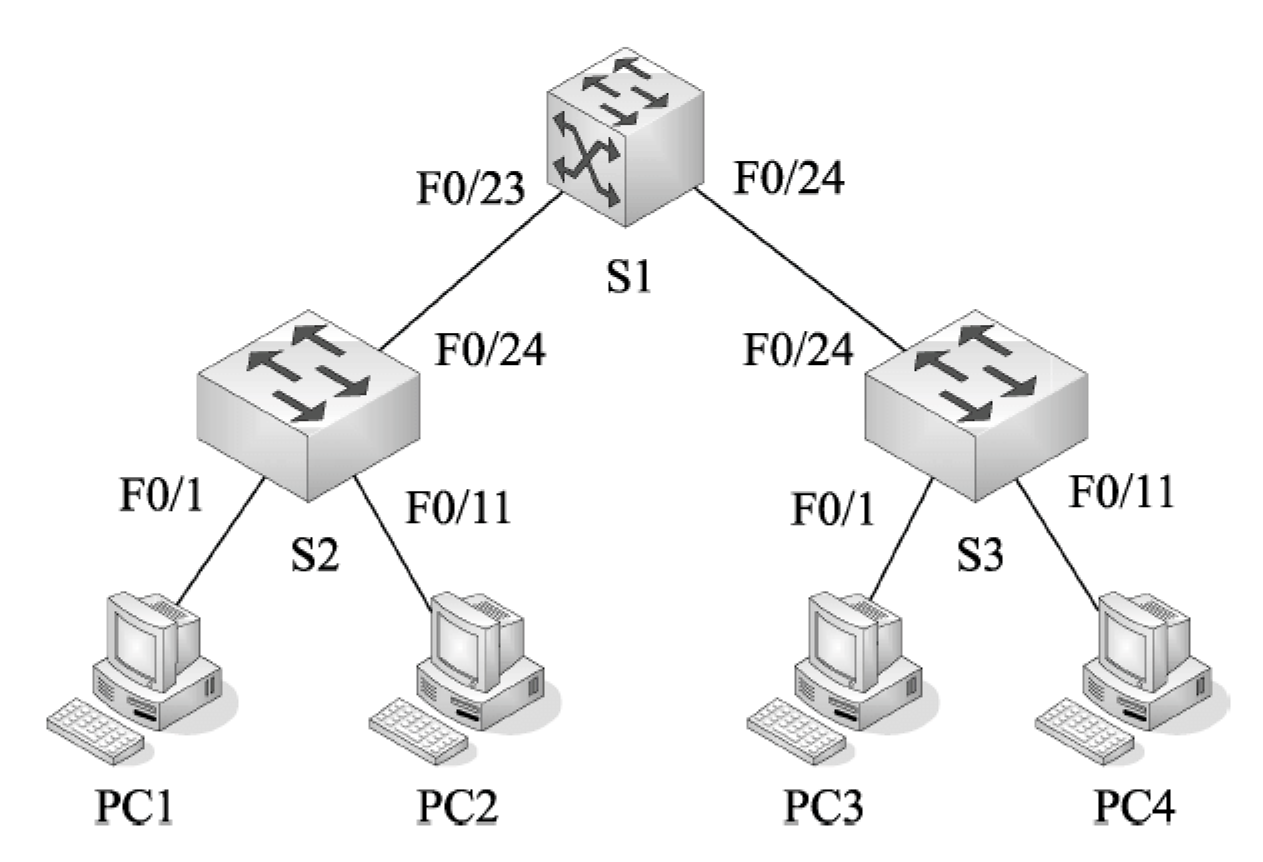



图 1-40　某单位网络拓扑结构

【问题 1】

由于业务需要，需将 PC1 和 PC3 划分在 VLAN10，PC2 和 PC4 划分在 VLAN20 中。IP 地址配置如表 1-15 所示，请将表 1-15 空白部分补充完整。

表 1-15　IP 地址配置

| 主机 | IP 地址 | 子网掩码 | 默认网关 | 定向广播地址 | 网络号 |
|---|---|---|---|---|---|
| PC1 | 192.168.0.1 | 255.255.254.0 | 192.168.0.254 | (1) | (2) |
| PC2 | 192.168.2.1 | 255.255.254.0 | 192.168.0.254 | (3) | (4) |
| PC3 | 192.168.2.1 | 255.255.254.0 | 192.168.0.254 | — | — |
| PC4 | 192.168.2.2 | 255.255.254.0 | 192.168.0.254 | — | — |

【问题 2】(3 分)

管理员计划使用 VTP 为网络划分 VLAN，为 S1 做了以下配置，请将其补充完整或解释命令：

```
Switch>
Switch>__(5)__;进入特权模式
Switch#config terminal
Switch(config)#__(6)__S1 ;命名
S1(config)#vtp mode__(7)__;设置为VTP服务器模式
S1(config)#vtp password class ;设置为__(8)__
S1(config)#vtp domain s1 ;设置为__(9)__
S1(config)#vlan 10
S1(config)#vlan 20
S1(config)#interface range fastethernet 0/23-24 ;进入多个接口配置模式
S1(config-if-range)#switchport mode trunk ;设置接口为中继模式
……
```

【问题 3】(4 分)

管理员为 S2 做了如下配置，请将其补充完整或解释命令：

```
……
S2(config)#vtp mode__(10)__;设置为VTP客户端模式
```

```
S2(config)#vtp password__(11)__;设置VTP口令
S2(config)#interface fastethernet 0/24
S2(config-if)#switchport mode__(12)__;设置接口为中继模式
S2(config)#interface fastethernet 0/1
S2(config-if)#switchport access vlan 10 ;__(13)__
S2(config)#interface fastethernet 0/11
S2(config-if)#switchport access vlan 20 ;__(14)__
```

**【问题4】(4分)**

由于业务扩展，需在S2上创建VLAN 30，管理员在S2上使用了以下命令：

```
S2(config)#vlan 30
VTP VLAN configuration not alloweD.
S2(config)#
```

使用show vlan命令查看后，发现VLAN30未创建成功，可能的原因是__(15)__。

(15)备选答案：

A. VLAN配置命令使用错误

B. VLAN配置模式错误

C. S2是client模式，不允许创建、删除和修改VLAN

D. S2不支持VLAN

**分析：**

**【问题1】**

广播地址分为定向广播地址和直接广播地址，其中定向广播地址是指将信息广播至指定的子网内的所有主机，这样的广播地址为二进制主机部分的位全1，而直接广播地址是全1的广播地址，即255.255.255.255。

网络号可使用IP地址与子网掩码二进制相“与”的方法进行计算。

**【问题2】和【问题3】**

题目中给出了交换机的3种模式进入的命令列表及VTP服务器模式的配置命令列表，需将S1配置为VTP服务器模式，并设置通信口令和域名等信息。VTP服务器模式的交换机可以将自身的VLAN配置信息以数据的形式发送给其他使用中继接口相连的交换机，为了安全起见，在通信时需使用配置的通信口令和域名进行验证，当口令和域名都一致时才可以进行正常通信，客户端交换机接收到服务器发来的VLAN配置信息，并将该信息应用于自身。

**【问题4】**

该问题考查的是VTP交换机3种模式的基本知识。

VTP技术中，交换机有3种模式。

服务器模式：在该模式下管理员可对交换机上的VLAN进行创建、修改、删除操作，并且可将VLAN配置信息以数据的形式发送至与之相连的其他交换机。

客户端模式：在该模式下管理员不能对交换机上的VLAN进行创建、修改、删除操作，交换机仅接收服务器发送给自己的配置信息，并应用于自身，交换机不转发这些信息。

透明模式：在该模式下管理员可对交换机上的VLAN进行创建、修改、删除操作，对于服务器发送给自己的VLAN配置信息，交换机不应用，仅将该信息转发至其他交换机。

根据题意描述，交换机 S2 所处的模式为客户机模式，管理员无法对交换机上的 VLAN 配置信息进行修改。

答案：

【问题 1】

(1) 192.168.1.255　　(2) 192.168.0.0

(3) 192.168.3.255　　(4) 192.168.2.0

【问题 2】

(5) enable　(6) hostname　(7) server　(8) 设置特权模式密码　(9) VTP 域名

【问题 3】

(10) client　　(11) class

(12) trunk　　(13) 将 f0/1 加入 VLAN 10

(14) 将 f0/11 加入 VLAN 20

【问题 4】

(15) C

**例 3**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2015 年 11 月下午试题一)

【说明】

某单位网络拓扑结构如图 1-41 所示，要求办公楼能与互联网物理隔离，所有汇聚交换机均采用三层交换机。

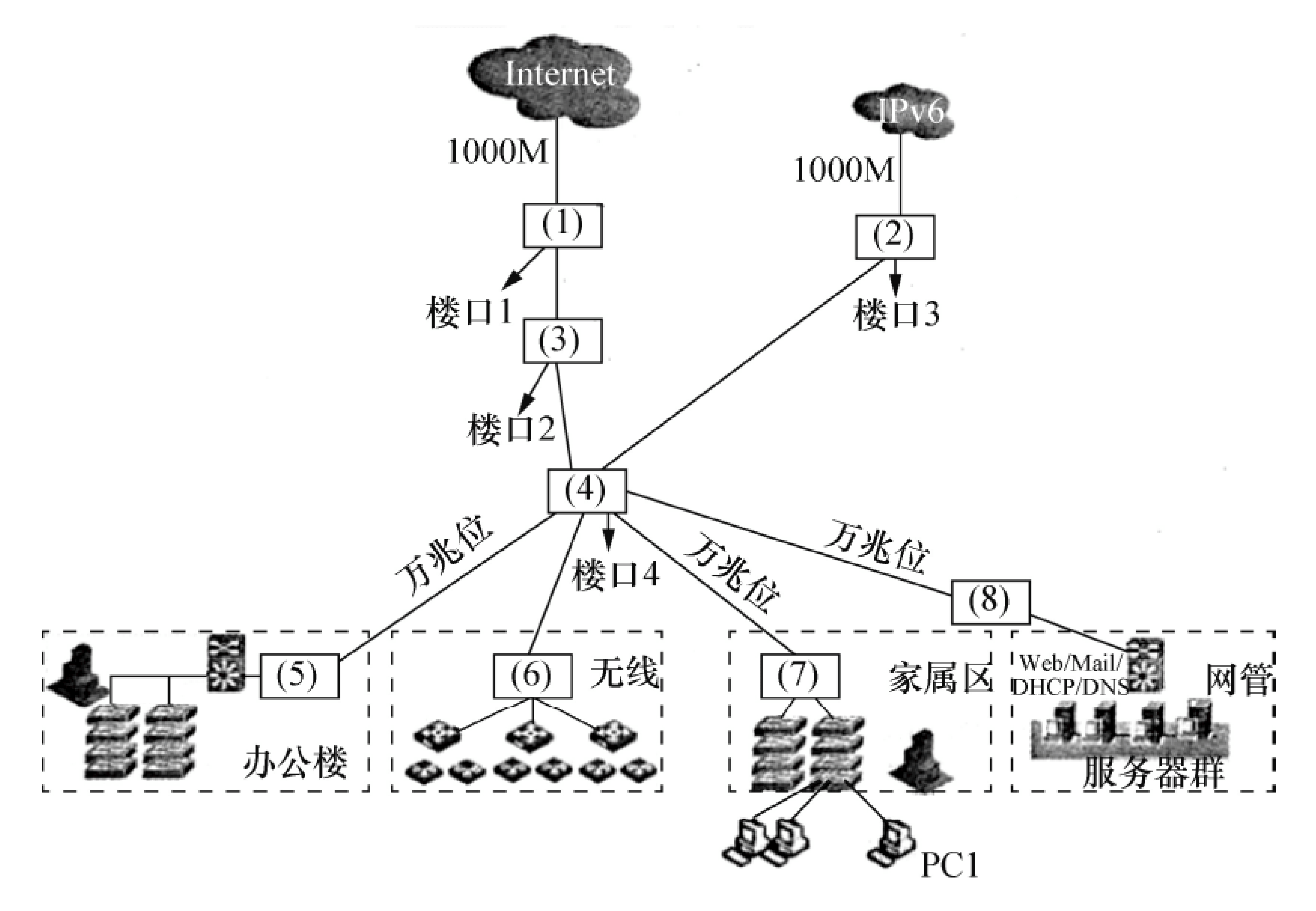



图 1-41　某单位网络拓扑结构

【问题 1】

请为图 1-41 中空缺处(1)～(8)选择合适设备(限选一次)。

(1)～(8)备选答案：

A．网闸　　　B．汇聚交换机　C．核心交换机
D．AP 控制器　E．出口路由器　F．IPv6 路由器
G．防火墙　　H．并发与流量控制器(采用桥接模式)

【问题 2】(4 分)

在 PC1 中运行 tracert www.aaa.com 命令后，显示结果下所示：

```
C:\Documents and Settings\User>tracert www.aaa.com
Tracing route to www.aaa.com [213.120.116.5]
Over a maximum of 30 hops:

  1    2ms    1ms    <1ms 10.174.255.254
  2    3ms    2ms    1ms  10.155.65.79
  3    <1ms   <1ms   <1ms 10.138.79.1
  4    21     19ms   19ms 123.126.0.218
  5    22ms   23ms   23ms 219.158.16.73
  6    18ms   18ms   18ms 61.150.156.138
  7    19ms   19ms   19ms 213.120.116.5

    Trace complete.
```

接口 1 的 IP 地址为 (9) ；接口 4 的 IP 地址为 (10) 。

【问题 3】(6 分)

在 PC 1 上运 route print 后得到 PC1 的路由信息，如图 1-42 所示。

```
C:\Documents and Settings\asus>route print
===========================================================================
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
      0.0.0.0          0.0.0.0          10.174.255.254   10.174.107.159   25
      10.174.0.0       255.255.0.0      10.174.107.159   10.174.107.159   25
      10.174.107.159   255.255.255.255  127.0.0.1        127.0.0.1        25
      10.255.255.255   255.255.255.255  10.174.107.159   10.174.107.159   25
      127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1        1
      224.0.0.0        240.0.0.0        10.174.107.159   10.174.107.159   25
      255.255.255.255  255.255.255.255  10.174.107.159   3                1
      255.255.255.255  255.255.255.255  10.174.107.159   10.174.107.159   1
Default Gateway:  10.174.255.254
===========================================================================
```

图 1-42　PC1 路由信息

请完善 PC1 的 Internet 协议属性参数。

IP 地址： (11) ；

子网掩码： (12) ；

默认网关： (13) 。

图 1-42 中第 1 条路由记录的作用是 (14) 。

**分析：**

**【问题 1】**

本问题考查设备的选择。通常出口处均是路由器，IPv4(图中(1)处)与 IPv6(图中(2)处)出口处分别是出口路由器和 IPv6 路由器；并发与流量控制器通常放在路由器之后、交换主干之前，故(3)处为并发与流量控制器；(4)处是交换核心，故采用核心交换机；办公楼与互

联网物理隔离，故(5)处为网闸；(6)处管理无线局域网接入故为 AP 控制器；(7)处的汇聚交换机以及(8)处的防火墙较为明显。

【问题 2】

接口 1 是经过 3 跳到达的网关，故地址为 10.138.79.1，接口 4 为 10.155.65.79。

【问题 3】

由第 3 条记录可以看出，PC1 的 IP 地址为 10.174.107.159，由第 1 条记录可以看出，PC1 的默认网关 IP 地址为 10.174.255.254，子网掩码为 255.255.0.0。第 1 条路由记录的作用是默认路由，即路由列表中无匹配记录时采用的转发路由。

答案：

【问题 1】

(1) E　(2) F　(3) H　(4) C　(5) A　(6) D　(7) B　(8) G

【问题 2】

(9) 10.138.79.1　(10) 10.155.65.79

【问题 3】

(11) 10.174.107.159

(12) 255.255.0.0　(13) 10.174.255.254

(14) 这表示发向任意网段的数据通过本机接口 10.174.107.159 被送往一个默认的网关 10.174.255.254，它的管理距离是 25。

**例 4**　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2016 年 5 月下午试题一)

【说明】

某网络拓扑结构如图 1-43 所示，路由器 R1 的路由信息以下：

```
C 202.118.1.0/24 is directly connected,FastEthernet0/0
R 202.118.2.0/24[120/1]via 192.168.112.2,00:00:09,Serial0
192.168.112.0/30 is subnetted,1 subnets
C 192.168.112.0 is directly connected,Serial0
```

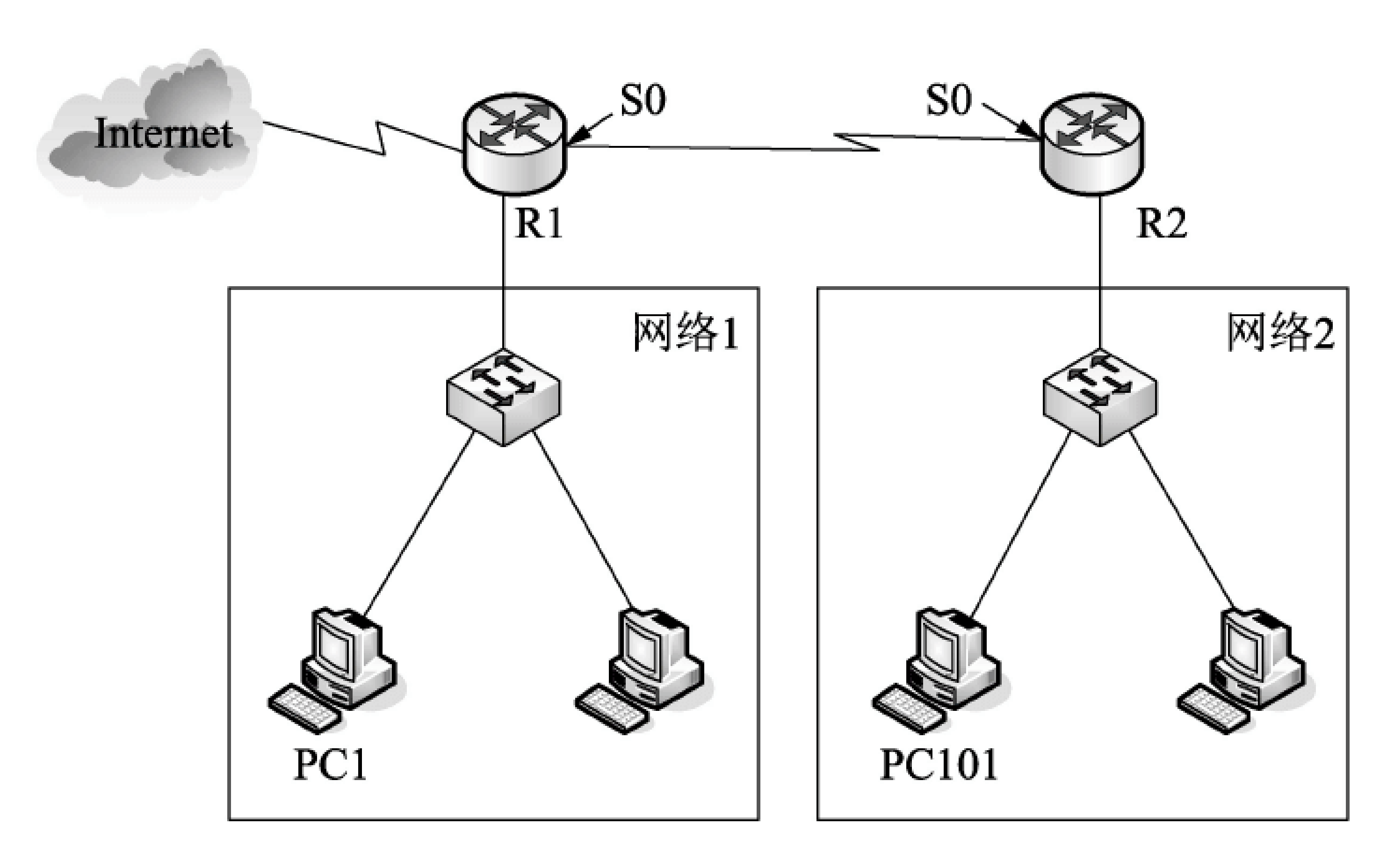



图 1-43　某网络拓扑结构

【问题 1】

路由器中查看路由的命令为 Router#__(1)__。

路由器 R1 接口 s0 的 IP 地址为__(2)__。

路由器 R2 接口 s0 的 IP 地址为__(3)__。

【问题 2】

为 PC1 配置 Internet 协议属性参数。

IP 地址：__(4)__；(给出一个有效地址即可)

网掩码：__(5)__；

为 PC101 配置 Internet 协议属性参数。

IP 地址：__(6)__；(给出一个有效地址即可)

子网掩码：__(7)__。

【问题 3】

若 PC1 能 ping 通 PC101，而 PC101 不能 ping 通 PC1，可能原因是__(8)__。

若 PC1 不能 ping 通 PC101，但可以和 PC101 进行 QQ 聊天，可能原因是__(9)__。

(8)、(9)备选答案：

A．PC101 上 TCP/IP 协议安装错误

B．R2 没有声明网络 2

C．R1 没有声明网络 1

D．PC101 上设置了禁止 ICMP 攻击

【问题 4】

填充表 1-16，完成路由器 R2 上网络 2 的用户访问 Internet 的默认路由。

图 1-16　答题表

| 目的网络 IP 地址 | 子网掩码 | 下一跳 IP 地址 | 接口 |
|---|---|---|---|
| (10) | (11) | (12) | (13) |

(10)～(13)备选答案：

A．0.0.0.0

B．255.255.255.255

C．202.118.1.0

D．192.168.112.1 或 R1 的 S0

E．192.168.112.2 或 R2 的 S0

**分析：**

【问题 1】

本问题重点考察路由表，查看 IP 地址配置。

(1) 路由器中，查看路由信息，使用命令 show ip route。

(2) 由图 1-40 可知，路由器 R1 的路由信息中网络 202.118.2.0/24 是通过 RIP 路由协议产生，下一跳为 192.168.112.2，故路由器 R1 接口 s0 的 IP 地址为 192.168.112.1；路由器 R2 接口 s0 的 IP 地址为 192.168.122.2。

【问题 2】

本问题重点考察主机 IP 地址配置。

由路由器路由记录可知，网络 202.118.1.0/24 与路由器 R1 直连，网络 202.118.2.0/24 不直接相连，通过 RIP 协议可达。结合拓扑结构可知，PC1 属于网络 202.118.1.0/24，PC101 属于网络 202.118.2.0/24

因此，PC1 IP 地址为 202.118.1.1～254，子网掩码为 255.255.255.0，PC101 IP 地址为 202.118.2.1～254，子网掩码为 255.255.255.0。

【问题 3】

本问题重点考察主机之间通信。

(1) 若 PC1 能 ping 通 PC101，而 PC101 不能 ping 通 PC1。首先若 PC101 上 TCP/IP 协议安装错误，PC1 是不能 ping 通 PC101 的，由此将 A 排除；其次 R1 的路由表上以显示 202.118.2.0/24，故 R2 声明了网络 2，由此将 B 排除；若 PC101 上设置了禁止 ICMP 攻击，PC1 是不能 ping 通 PC101 的，由此排除 D；若 R1 没有声明网络 1，网络 1 与 R1 直连，其能看到网络 1，R2 看不到网络 1，故 PC101 不能 ping 通 PC1，C 正确。

(2) 若 PC1 不能 ping 通 PC101，但是可以和 PC101 进行 QQ 聊天。PC101 上 TCP/IP 协议安装错误、R2 没有声明网络 2、以及 R1 没有声明网络 1 都不成立，只有 PC101 上设置了禁止 ICMP 攻击正确，答案 D。

【问题 4】

本问题重点考察默认路由。

默认路由是缺省路由，即路由器中已有路由均匹配不上来时采用的路由。目的网络 IP 地址和子网掩码均为 0.0.0.0，路由器 R2 上网络 2 的用户访问 Internet 的默认路由，经过 R2 接口 S0(192.168.112.2)，下一跳为 R1 的接口 S0(192.168.112.1)。

**答案：**

【问题 1】

(1) show ip route

(2) 192.168.112.1

(3) 192.168.112.2

【问题 2】

(4) 202.118.1.1～254　　(5) 255.255.255.0

(6) 202.118.2.1～254　　(7) 255.255.255.0

【问题 3】

(8) C　　(9) D

【问题 4】

(10) A　(11) A　(12) D　(13) E

**例 5**　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2016 年 11 月下午试题三)

【说明】

某公司网络拓扑结构图如图 1-44 所示，其中 S1 为三层交换机。

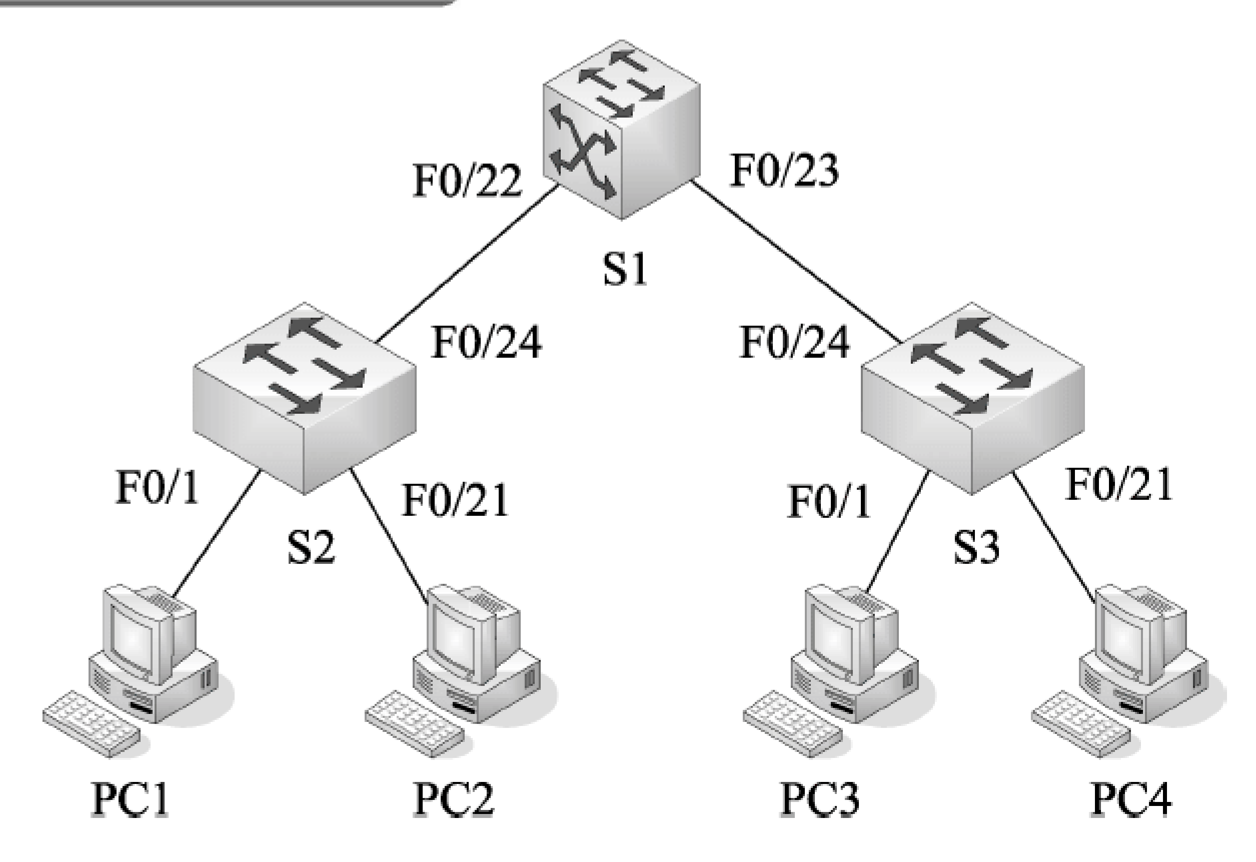



图 1-44　某单位网络拓扑结构

**【问题 1】**

由于公司分为多个部门，网管员决定为公司各部门分别划分不同的 VLAN。为便于管理，网管员应采用__(1)__方法划分 VLAN。如图 1-44 所示，PC1 和 PC3 处于 VLAN10，PC2 处于 VLAN20，PC4 处于 VLAN40，PC1 发送的广播数据包__(2)__能收到。

为了实现公司全网互通，需实现 VLAN 间通信，应在__(3)__或者三层交换机上实现，以上两种设备工作在 OSI 的__(4)__。

备选答案：

(1) A．基于 IP 地址　　B．基于交换机端口
　　C．基于 MAC 地址　　D．基于不同用户

(2) A．仅 PC3　　B．PC2 和 PC4
　　C．仅 PC2　　D．PC3 和 PC4

(3) A．路由器　　B．网桥　　C．HUB　　D．防火墙

(4) A．物理层　　B．数据链路层　　C．网络层　　D．传输层

**【问题 2】**

网管员对交换机完成了基本配置，基本配置代码如下，请将下面配置代码或注释补充完整。

```
Switch>
Switch>__(5)______//进入特权模式
Switch#config__(6)__  //进入配置模式
Switch(config)#hostname__(7)__    //为交换机命名为 S2
S2(config)#interface fastEtheniet 0/24
S2(config-if-range)#switchport mode trunk    //__(8)__
S2(config)#mterface__(9)__fastEthernet 0/1-10
S2(config-if-range)#switchport access vlan 10//__(10)__
S2(config)#mterface ran ge'fastEthernet 0/11-23
S2(config-if-range)#switchport access__(11)__20
S2(coiifig if-range)#__(12)__     //退出到特权模式
S2#
……
```

S3 配置与 S2 同，略去。

**【问题 3】**

公司划分了 VLAN 10、VLAN20 和 VLAN 30 这 3 个 VLAN，其中 3 个 VLAN 的网关分别为 192.168.10.254/24、192.168.20.254/24 和 192.168.30.254/24。为实现 VLAN 间通信，需对三层交换机 S1 进行相应配置，配置代码如下。请将下面配置代码或注释补充完整。

```
行号  代码
 1   S1>enalb
 2   S1#config terminal
 3   S1(config)#interface___(13)___10      //进入 VLAN10 接口
 4   S1(config-if)#address___(14)___255.255.255.0      //配置 VLAN10 网关地址
 5   S1(config-if)#no shutdown
 6   S1(config-if)#exit          //___(15)___
 7   S1(config)#ip routing       //___(16)___
 8   S1(config)#
```

在上面的代码中，第___(17)___行代码是可以省略的。

(17)备选答案：

A．2　　B．4　　C．5　　D．7

**【问题 4】**

完成以上配置后，测试发现 PC1 可以与 PC2 通信，但无法与 PC3 和 PC4 通信，PC3 和 PC4 均无法 ping 通其各自网关地址。最可能的原因是___(18)___。

(18)备选答案：

A．VLAN 间路由配置错误　　B．网关 IP 地址配置错误

C．S1 至 S3 间链路类型配置错误　　D．VLAN 划分错误

**分析：**

**【问题 1】**

该问题考查考生对于 VLAN 的基本功能和基本知识的掌握程度。网络管理员可根据用户端的 IP 地址、交换机端口、MAC 地址等划分 VLAN，其中基于 IP 地址和 MAC 地址属于动态 VLAN 划分方法，该方法便于用户在不同的物理位置访问网络，但不便于网络管理员管理，基于交换机端口划分 VLAN 是一种静态 VLAN 划分方法，一旦划定 VLAN 成员将不会发生变化，便于管理员管理网络。

处于同一个 VLAN 的终端，可以直接互相通信，而处于不同 VLAN 的终端，则需要在 3 层设备上做相应的设置才能够相互通信。

**【问题 2】**

该问题考查考生对于 VLAN 配置的掌握程度。根据题意，规划 VLAN 的设置方法和设置项，并将配置代码或者解释补充完整。

为使不同的 VLAN 能够通过交换机端口，须将级联接口设置为中继(Trunk)模式，VLAN 创建后，将相应的端口放入指定 VLAN。最后使用 “end” 命令退出 VLAN 配置模式。

**【问题 3】**

该问题考查考生对于三层交换机上实现 VLAN 间通信的配置方法掌握程度。在三层交换机上创建 SVI(Switch Virtual Interface)交换机虚拟接口，并为其配置 IP 地址，开启三层交换机的路由功能即可。

需要注意的是，当在三层交换机上创建了 SVI 接口后，该接口自动处于 UP 模式，无须手工打开，因此，配置代码中的第 5 行为多余命令。

**【问题 4】**

该问题考查考生对于 VLAN 间路由配置故障定位和排除的掌握程度。根据题干说明，处于不同 VLAN 的 PC1 和 PC2 可以相互通信，而处于不同 VLAN 的 PC3 和 PC4 不能相互通信，且无法 ping 通其他各自网关地址。该故障说明 PC3 与 PC4 无法与其网关地址通信，而它们的网关地址均处于三层交换机(S1)的 SVI 接口上，即数据包无法到达 S1。考虑到 PC3 和 PC4 处于不同的 VLAN，要使得它们的数据包通过，级联接口需要设置为中继模式(Trunk)，可用排除法得到答案。

**答案：**

**【问题 1】**

(1) B　(2) A　(3) A　(4) C

**【问题 2】**

(5) enable　(6) terminal/t　(7) S2　(8) 配置中继模式

(9) range　(10) 进入 vlan10　(11) vlan　(12) end

**【问题 3】**

(13) vlan　(14) 192.168.10.254　(15) 退出接口配置模式

(16) 开启路由功能　(17) C

**【问题 4】**

(18) C

## 1.6.3　同步练习

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

**【说明】**

某公司上网用户较少(约 50 台上网机器)，因此公司网管申请了公网 IP 地址(117.112.2.101/30)，拟通过 NAT 方式结合 ACL 提供公司内部员工上网，公司内网 IP 地址段为 192.168.1.0/24。

该公司的网络拓扑结构如图 1-45 所示。

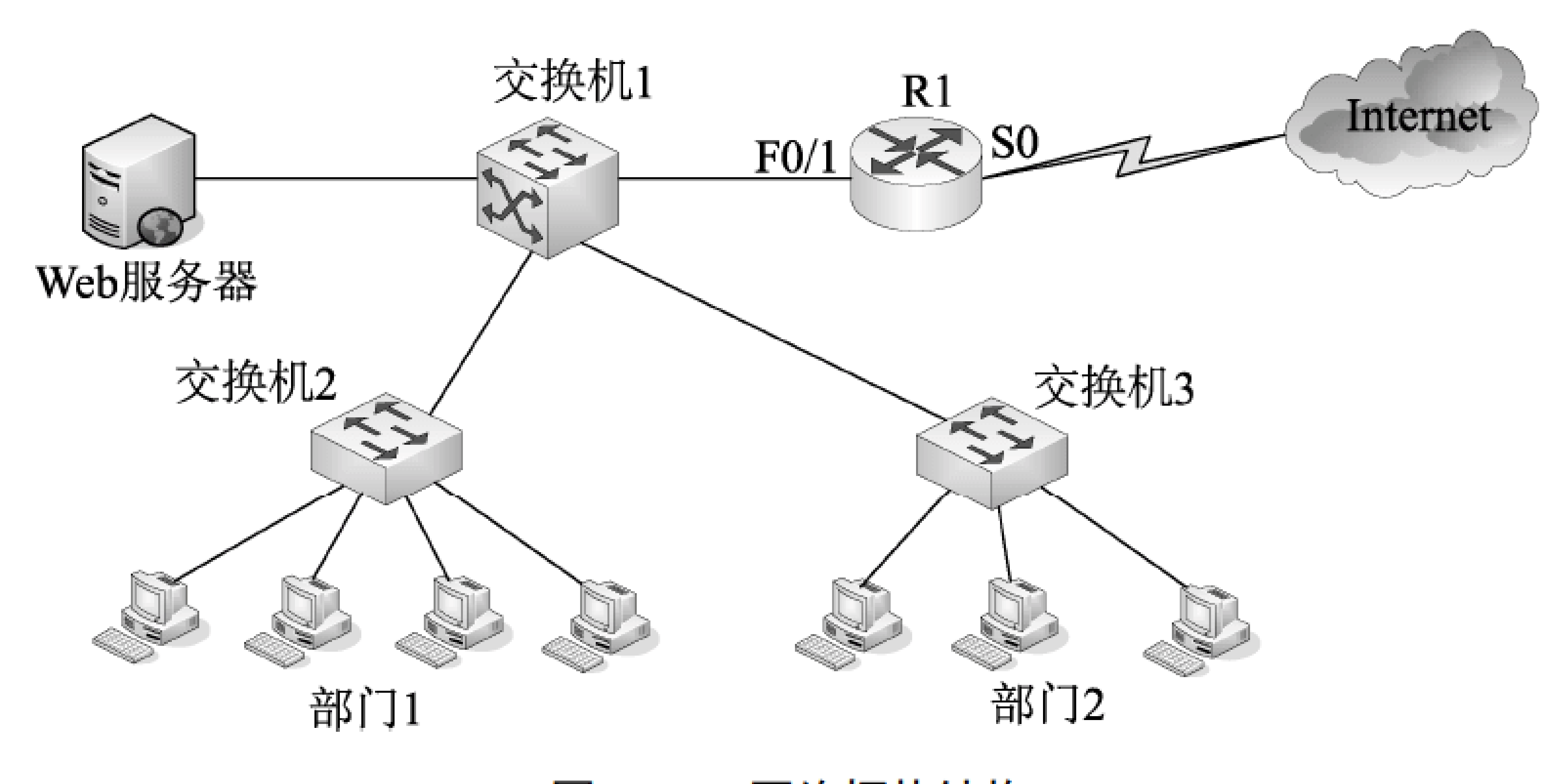



图 1-45　网络拓扑结构

【问题 1】

通过命令行接口(CLI)访问路由器有多种模式，请补充完成图 1-46 中(1)~(5)的相关内容，实现这四种模式的转换。

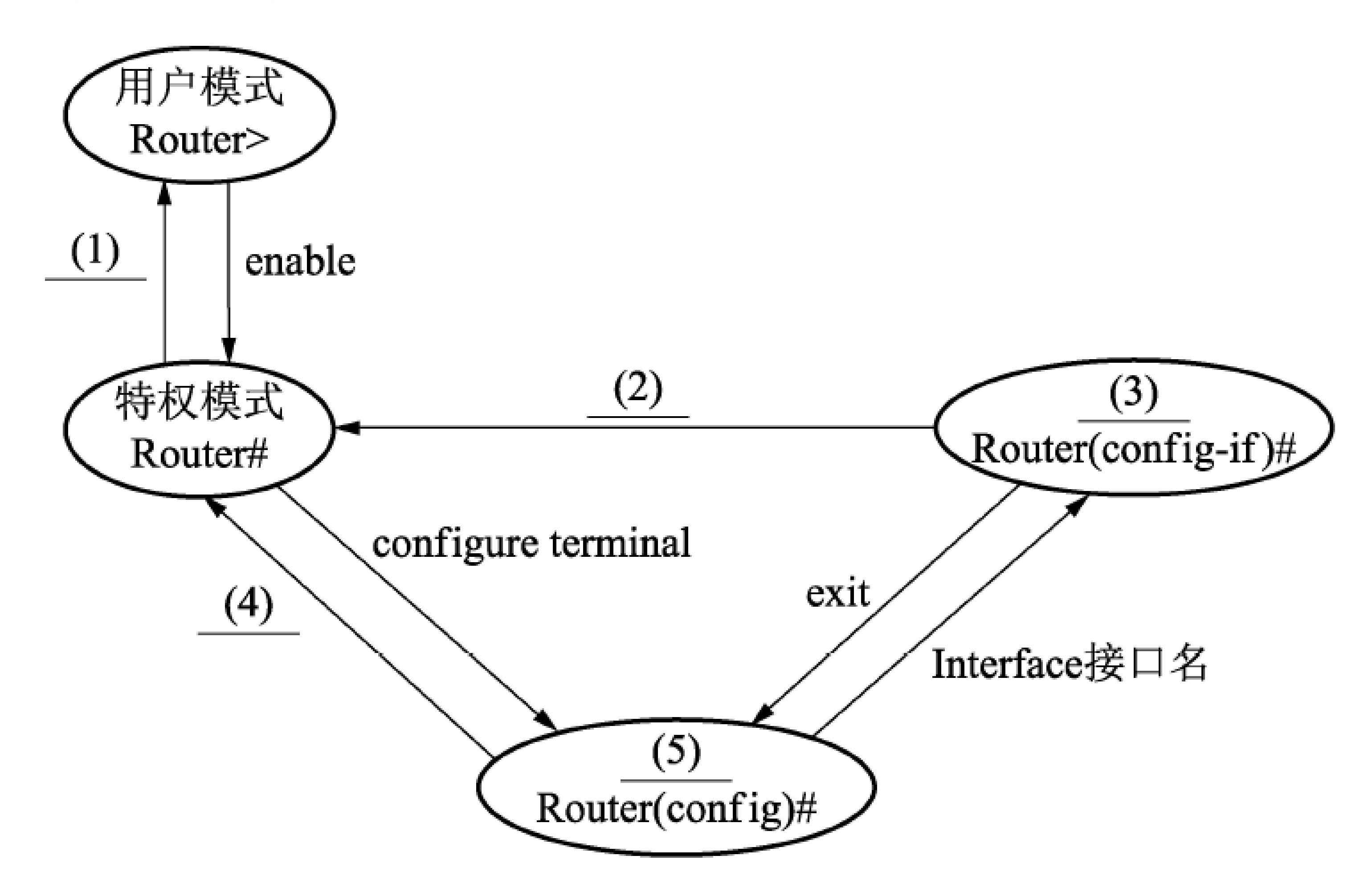



图 1-46　某单位网络拓扑结构图

【问题 2】

为了完成对路由器 R1 的管理，按照题目要求对路由器 R1 进行相关配置，请补充完整下列配置命令。

```
Router(config) # __(6)__
R1(config)# enable password abc001  //配置全局配置模式的明文密码为“abc001”
R1(config)# interface f0/1
R1(config-if)#ip address 192.168.1.1  255.2 5 5.255.0   //为 F0/1 接口配置 IP 地址
R1(config-if) # __(7)__      //激活端口
R1(config-if) #interface s0   //进入 s0 的接口配置子模式
R1(config-if) #ip address __(8)__  //为 s0 接口配置 IP 地址
……

R1( config )# line vty04
R1(config-line)# login
R1(config-line)# password abc001    //配置 vty 口令为“abc001”
……
R1(config)# __(9)__  //进入 Console 口的配置子模式
R1(config-line)# login
R1(config-line)# password abc001   //配置 Console 控制口口令为“abc001”
……
R1(config) # __(10)__ password-encryption   //为所有口令加密
R1# __(11)__ running-config    //查看配置信
```

【问题 3】

为实现该公司员工通过出口设备访问互联网的需求，必须在路由器 R1 上配置基于端口的动态地址转换，也就是 PAT，请解释或完成下列配置命令。

```
……
R1(config) # ip route 0.0.0.0  0.0.0.0  s0   // __(12)__
R1(config)# access-list 1 permit ip 192.168.1.0  0.0.0.255  // __(13)__
R1(config)# ip nat pool public 117.112.2.101  117.112.2.101  netmask
255.255.255.0
R1(config)# ip nat inside source list 1 pool public   //定义 NAT 转换关系
R1(config)# interface __(14)__
R1(config-if)# ip nat inside
R1(config)# interface __(15)__
R1(config-if)# ip nat outside   //定义 NAT 的内部和外部接口
……
R1# show ip nat transWions  //显示 NAT 转换表
R1# show ip nat statistics  //显示当前 NAT 状态
R1# write  // __(16)__
R1# reload  // __(17)__
……
```

**【问题 4】**

随着公司内部网络的不断扩大，为了公司内网的安全，可利用__(18)__快速实现企业内网的 VLAN 配置以解决广播风暴的问题，同时可使用__(19)__解决网络中的地址冲突以及地址欺骗等现象。

如果要实现外网用户对公司的 Web 服务器的访问，可利用__(20)__在 R1 上实现。随着公司规模的扩大，Web 服务器的访问量也会增大，这时也可将该网站托管。

### 1.6.4 同步练习参考答案

**【问题 1】**

(1) exit (2) end (3) 接口配置模式 (4)exit (5) 全局配置模式

**【问题 2】**

(6) hostname Rl (7) no shutdown (8) 117.112.2.101 255.255.255.252

(9) line console 0 (10) service (11) show

**【问题 3】**

(12) 配置通向 Internet 的默认路由

(13) 创建访问控制列表，定义需要转换的内网网段

(14) F0/1 (15) S0 (16) 保存配置信息 (17) 重新加载

**【问题 4】**

(18) VTP (19) IP 和 MAC 地址绑定 (20) 静态 NAT 转换

## 1.7 本 章 小 结

本章知识点在 2009 年的新大纲中变化较大，增加了交换机和路由器的配置以及网络接入服务知识点，弱化了综合布线的考核要求。

这部分内容主要要求考生掌握局域网的设计步骤、局域网的设备选型、综合布线、交换机的部署和配置、子网的划分方法以及综合布线系统的设计。要求考生综合上述知识，根据用户需求，合理利用局域网设备和技术设计出符合用户需求的网络。

本章内容为下午科目的重点内容，尤其是 Internet 协议属性配置、交换机的配置和路由器的配置，在以往的试题中曾多次考到。

# 1.8　达标训练题及参考答案

## 1.8.1　达标训练题

1．阅读以下说明，回答问题 1 至问题 3，将答案填入对应的答案栏内。

**【说明】**

某单位有一个网络，其中有一台主机的 IP 地址是 190.190.147.134。请回答以下问题。

**【问题 1】**这个地址是一个什么类型的地址？不划分子网时其网络地址是什么？广播地址是什么？

**【问题 2】**它的默认子网掩码是什么？

**【问题 3】**若子网掩码是 255.255.240.0，则这台主机所在的子网地址是什么？该子网的广播地址是什么？这个 IP 地址所在的子网的主机 IP 地址范围是什么？

2．阅读以下说明，回答问题 1 至问题 4，将解答填入对应的答案栏内。

**【说明】**

某公司申请了一个 C 类地址 196.102.56.0，公司有生产部门、市场部门、财务部门、人事部门、技术部门和经理办公室，每个部门都需要划分为单独的网络，即需要划分至少 5 个子网，每个子网至少支持 24 台主机(使用固定子网掩码)。

**【问题 1】**将子网掩码设置为什么？

**【问题 2】**每个子网有多少个主机地址？

**【问题 3】**196.102.56.197 所在子网的网络地址是什么？

**【问题 4】**196.102.56.197 所在子网的广播地址是什么？

3．阅读以下说明，回答问题 1 至问题 3，将解答填入对应的答案栏内。

**【说明】**

某一小型公司从 ISP 申请了一个 Internet 出口，ISP 给该公司提供了 5 个 IP 地址，分别是 222.34.109.66～222.34.109.70，ISP 给该公司提供的路由器地址是 222.34.109.65。

**【问题 1】**由于 ISP 忘记了告诉子网掩码，你认为最有可能的子网掩码是什么？

**【问题 2】**这个子网的子网地址是什么？

**【问题 3】**这个子网的广播地址是什么？

## 1.8.2 参考答案

1.

**【问题 1】**B 类地址、190.190.0.0、190.190.255.255

**【问题 2】**255.255.0.0

**【问题 3】**190.190.144.0、190.190.159.255、190.190.144.1～190.190.159.254

2.

**【问题 1】**255.255.255.224

**【问题 2】**30

**【问题 3】**196.102.56.192

**【问题 4】**196.102.56.223

3.

**【问题 1】**255.255.255.248

**【问题 2】**222.34.109.64

**【问题 3】**222.34.109.71

# 第 2 章　局域网服务器的安装和配置

大纲要求：

- IP 地址、子网掩码的规划配置。
- Windows Web 服务器的配置和维护。
- Windows DNS 服务器的配置和维护。
- Windows 电子邮件服务器的配置和维护。
- Windows FTP 服务器的配置和维护。
- Windows 代理服务器的配置和维护。
- Windows DHCP 服务器的配置和维护。

## 2.1　操作系统的安装

### 2.1.1　考点辅导

#### 2.1.1.1　Windows Server 2008 R2 安装程序

Windows Server 2008 R2 是 Windows Server 2008 的升级产品，为一款仅支持 64 位的操作系统，可以为大、中或小型企业搭建功能强大的网站和应用程序服务器平台。强大的管理功能与经过强化的安全措施，简化了服务器的管理，提高了资源的可用性，有效保护企业应用程序和数据。另外提供了全新的虚拟化技术，提供更多的高级功能，在改善 IT 效率的同时提高了灵活性。无论是整合服务器，构建私有云，或提供虚拟桌面基础架构(VDI)，强大的虚拟化功能，可以将数据中心与桌面的虚拟化战略提升到一个新的层次。

1. Windows Server 2008 R2 的新增功能

Windows Server 2008 R2 增强了核心 Windows Server 操作系统的功能，提供了富有价值的新功能，以协助各种规模的企业提高控制能力、可用性和灵活性，适应不断变化的业务需求。新的 Web 工具、虚拟化技术、可伸缩性增强和管理工具有助于节省时间、降低成本，并为信息技术(IT)基础结构奠定坚实的基础。

Windows Server 2008 R2 包含了许多增强功能，从而使该版本成为有史以来最可靠的 Windows Server Web 应用程序平台。该版本提供了最新的 Web 服务器角色和 Internet 信息服务 IIS7.5 版，并在服务器核心提供了对.NET 更强大的支持。IIS 7.5 的设计目标着重于功能改进，使网络管理员可以更轻松地部署和管理 Web 应用程序，以增强可靠性和可伸缩性。另外，IIS 7.5 简化了管理功能，并为自定义 Web 服务环境提供了比以往更多的方法。

2. Windows Server 2008 R2 的安装

Windows Server 2008 R2 家族包括 Windows Server 2008 R2 基础版、Windows Server

2008 R2 标准版、Windows Server 2008 R2 企业版、Windows Server 2008 R2 数据中心版、WindowsServer 2008 R2 Web 版等产品，安装时用户可以进行选择。安装时系统的硬件环境建议 CPU 主频在 1.4 GHz(x64 处理器)以上，内存 512MB 以上，硬盘 32GB 以上，监视器的分辨率在 800 像素×600 像素以上。

Windows Server 2008 R2 的安装继承了 Windows 产品安装时方便、快捷、高效的特点，几乎不需要多少人工参与就可以自动完成硬件的检测、安装、配置等工作。用户需要做的仅是通过屏幕来了解它所提供的各项新技术以及产品特点。安装过程中会收集区域信息、语言信息、个人注册信息、计算机 / 管理员基本信息、网络基本信息等。

3. Windows Server 2008 R2 的基本配置。

1) 本地用户和组

为了保障计算机与网络的安全，Windows Server 2008 R2 为不同的用户设置了不同的权限，同时通过将具有同一权限的用户设置为一个组来简化对用户的管理。

组是从 Windows NT 系统继承下来的安全管理形式，是指多个对象的集合，对象可包括用户、计算机、联系人及其他组。组账户是用户账户的集合，包括了那些具有相同权限的用户账户。当某个用户成员加入一个组时，则该用户也将被赋予该组具有的所有权限。用户也可以同时属于多个组，并且拥有他所加入组的所有权限。组文件夹中的默认组有 Administrator、Backup Operator、Guests、HelpServicesGroup、Network Configuration Operator、Performance Log Users、Performance Monitor Users、Power Users、Print Operators、Remote Desktop Users、Replicator、TelnetClients、Users。

2) 配置网络协议

只有在计算机上正确安装网卡驱动程序和网络协议，并正确设置 IP 地址信息之后，服务器才能与网络内的计算机进行正常通信。

正确安装网卡驱动和网络协议，并正确配置 IP 地址信息是服务器与计算机进行正常通信的基础。配置网络协议主要是指配置 TCP/IP 协议，包括 IP 地址、子网掩码、默认网关、DNS 和 WINS 等。具体操作为：依次执行“开始”→“控制面板”→“网络连接”→“本地连接”命令，打开“本地连接 状态”对话框，单击“属性”按钮；打开“本地连接 属性”对话框，选中“Internet 协议(TCP/IP)”选项，单击“属性”按钮；打开“Internet 协议版本 4(TCP/IPv4)属性”对话框，然后进行设置，如图 2-1 所示。

3) 添加、删除和管理服务器角色

安装 Windows Server 2008 R2 时，在默认的情况下并不安装任何网络服务，要提供网络服务，必须添加相应的服务器角色，如 DNS 服务器、远程桌面服务、文件服务等。

4. 远程管理

1) Windows Server 2008 R2 远程桌面服务

终端服务提供通过作为终端仿真器工作的“瘦客户”软件远程访问服务器桌面的能力。终端服务基本由 3 部分技术组成：客户端部分、协议部分及服务器部分。在客户端安装名为“远程桌面”的程序后，就可以看到服务器完全一致的计算机桌面，并能执行一样的操作。犹如将服务器搬到自己眼前一样。客户端和服务器通过远程桌面协议进行通信。




图 2-1　“Internet 协议版本 4(TCP/IPv4)属性”对话框

在 Windows Server 2008 R2 中，终端服务也没有被默认安装，需要用户手动添加。具体操作步骤为：依次执行“开始”→“管理工具”→“配置您的服务器向导”命令，在打开的“配置您的服务器向导”对话框中，单击“下一步”按钮；按照“预备步骤”窗口中的说明操作，单击“下一步”按钮；在“服务器角色”对话框中，选择“终端服务器”选项，单击“下一步”按钮；按照向导中的说明操作来完成安装。

默认情况下只有系统管理员组用户(Administrators)和系统组用户(System)拥有访问和完全控制终端服务器的权限，另外远程桌面用户组(Remote Desktop Users)的成员只拥有访问权限而不具备完全控制权。而在很多时候，默认的权限设置往往并不能完全满足实际需求，因此还需要赋予某些特殊用户远程连接的权限。具体操作为：依次执行“开始”→“管理工具”→“终端服务配置”命令，在打开的“终端服务配置”对话框中，双击右侧窗格中的“RDP-Tcp”连接。打开“RDP-Tcp 属性”对话框，切换到“权限”选项卡，如图 2-2 所示。“权限”选项卡中可以设置有哪些用户和组可以从客户端登录该终端服务器。




图 2-2　“权限”选项卡

2) Windows Server 2008 R2 远程管理

远程管理的使用与活动目录和组策略的使用一样重要，是衡量 Windows Server 2008 R2 网络管理员、系统管理员水平的重要指标。

在 Windows Server 2008 R2 家族操作系统中，进行远程管理的方法是多种多样的，主要包括 MMC(微软管理控制台)法、远程桌面连接法、管理远程桌面(终端服务)法、管理工具方法、远程协助法、Telnet 法、远程管理 Web 法和远程存储法。

3) Microsoft 管理控制台(MMC)

Microsoft 管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具。但 MMC 不执行管理功能，可以使用 MMC 创建、保存并打开管理工具单元，这些管理工具用来管理软件、硬件和 Windows 系统的网络组件。

使用 MMC 有以下两种方法。

(1) 在用户模式中使用已有的 MMC 控制台管理系统。

(2) 创建新控制台或修改已有的 MMC 控制台。

4) 远程桌面连接

(1) 配置远程桌面连接。

要想成功连接到终端服务器，必须保证服务器允许进行“远程桌面”连接。右击“我的电脑”，在弹出的快捷菜单中选择“属性”命令，打开“远程”选项卡，选中“允许用户远程连接到您的计算机”复选框。

(2) 使用桌面连接。

用户要想远程连接到终端服务器，首先需要安装客户端。安装完客户端后执行以下操作就可以连接到终端服务器。

依次执行“开始”→“所有程序”→“附件”→“远程桌面连接”命令，在打开的“远程桌面连接”对话框中，单击“选项”按钮，切换到登录设置对话框，如图 2-3 所示。输入终端服务器的 IP 地址、用户名、密码，并单击“连接”按钮。出现 Windows 登录对话框后输入已授权的用户名的密码即可完成连接。




图 2-3 运行远程访问服务

#### 2.1.1.2　安装 Red Hat Enterprise Linux

Linux 发行版本趋于多样化。目前在操作系统核心(Kernel)部分，常用的版本是 4.x.x。为了方便安装，将操作系统核心与各种软件组合起来一起包装，作为 Linux 的发行版本，目前市场上已经有 300 多种发行版本，如 Red Hat Linux、Slackware Linux、Open Linux、Informagic、SuSE Linux、Debian Linux、Redflag Linux、Turbo Linux、Linux-Mandrake 和红旗 Linux 等。

Red Hat Linux 是目前流行最用 RPM(Red Hat Package Manager)的方式，将软件以套件的形式分门别类地进行整理，供用户使用。

Red Hat 于 2014 年 6 月 9 日正式发布 Enterprise Linux 7 以来，已经更新至 Enterprise Linux 7.3 版本。该版本内核为 Kernel 3.10，它在 RHEL 6 的基础上又有了很大的改进，集成了应用程序虚拟化技术 Docker 和对 systemd 进程管理器的支持，XFS 成为 RHEL 7 默认的文件系统以及能监控系统 PCP 等新功能特性，使之较 RHEL 6 在功能和性能方面有很大提升。

1. Red Hat Enterprise Linux 7 的安装

Red Hat Enterprise Linux 7 图形化安装程序引入了一个全新的用户界面设计，使安装方便、快捷。新的安装程序界面将一组配置选项放到了一个中心界面，用户单击需要改变的选项，改变它们，然后开始安装。

1) 选择系统引导方式

首先在计算机的 CMOS 中把启动盘的先后顺序设置好，然后把安装光盘放入光驱，重新启动计算机，此时，系统会进行自检，自检完毕后会出现安装系统的引导界面。

这个屏幕包括如下引导选项：

- Install Red Hat Enterprise Linux 7.0　(安装 RHEL 7.0)
- Test this media & install Red Hat Enterprise Linux 7.0　(测试安装文件并安装 RHEL 7.0)
- Troubleshooting　(修复故障)

一般情况下选择第一项，然后按 Enter 键进入引导安装。

2) 配置分区

(1) 分区的命名。

Linux 通过字母数字的组合来识别硬盘分区。命名规则如下。

前两个字母表示分区所在的设备类型，hd 表示 IDE 硬盘，sd 表示 SCSI 硬盘。

第三个字母表示分区在哪个设备上，hda 表示在第一块 IDE 硬盘上，hdb 表示在第二块 IDE 硬盘上，sdc 表示在第三块 SCSI 硬盘上。

数字表示分区的次序，1～4 表示主分区或扩展分区，逻辑分区从 5 开始。

(2) 分区的组织。

Linux 系统支持多分区结构，各个分区的功能如表 2-1 所示。

Linux 系统对分区的基本要求如下。

① 至少有一个根(0 分区)用来存放系统文件及程序。其大小至少在 SGB 以上。

② 要有一个 SWAP(交换)分区，它的作用相当于 Windows 里的虚拟内存，swap 分区的大小一般为物理内存容量的 1.5 倍(内存<8G)。当系统物理内存大于 8G 时，swap 分区配

置8～16G即可，太大无用，浪费磁盘空间。

③ /boot分区，这是Linux系统的引导分区，用于存放系统引导文件，所以一般设置100～200M即可。

表2-1 分区功能

| 分 区 | 功 能 |
|---|---|
| / | 整个系统的基础(必备) |
| swap | 操作系统的交换空间(必备) |
| /boot | 在根下创建，用来单独保存系统引导文件 |
| /usr | 用来保存系统软件 |
| /home | 包含所有用户的主目录，可保存几乎所有的用户文件 |
| /var | 保存邮件文件、新闻文件、打印队列和系统日志文件 |
| /tmp | 用来存放临时文件 |

这里我们按照企业中最常用到的针对网站集群架构中的某个节点服务器场景进行分区，该服务器上的数据有多分区(其他节点也有)且数据不太重要。

- /boot:设置为200MB。
- Swap：物理内存的1.5倍，本机内存8GB，所以设置为12GB。
- /：剩余硬盘空间大小，这就相当于Windows中只有一个C盘，所有数据和系统文件都放在一起。

2. Red Hat Enterprise Linux 7的使用

1) 系统启动、关闭等基本操作

(1) 启动系统。

Red Hat Enterprise Linux 7是通过GRUB2来引导系统的，如果计算机装有多个操作系统，一般只要在Red Hat Enterprise Linux 7安装过程中进行了正确的配置，GRUB2都会在引导界面上显示系统列表，供用户选择进入哪一个系统；如果不选择，系统会在规定的时间后自动进入默认的系统。假如引导系统列表中有多个操作系统，可以通过按下或上键进行选取，选定后按Enter键即可。如果是第一次运行该系统，系统将自动进入“欢迎”界面，一般来说，在系统执行自检完成之后，系统将进入Red Hat Enterprise Linux 7的登录界面。

(2) 用reboot命令重新启动计算机。

一般情况下，按Ctrl+Alt+Del组合键可以重新启动计算机，但是正规的用法是执行reboot命令，其语法为：

```
reboot [-n] [-w] [-d] [-f] [-i]
```

(3) 用shutdown命令关机或进入单人维护模式。

利用shutdown命令可以关闭系统中正在运行的所有程序，并可以根据用户的需要进入单人系统维护模式，或执行重开机、关机的操作。shutdown命令的语法如下：

```
shutdown [-t secs] [-rkhncfF] time [warning message]
```

2)　文本模式和图形化模式的切换

在文本模式下，输入 startx 命令可以直接进入 X WindowSystem 界面。而在 X WindowSystem 界面下，也可以使用文本模式。

Linux 主机在控制台(Console)下提供了 6 个虚拟终端，在每一个虚拟终端中都可以执行各自的程序，如表 2-2 所示。

表 2-2　控制台、组合键和内容

| 控 制 台 | 组 合 键 | 内　叠 |
|---|---|---|
| 1 | Ctrl+Alt+F1 | X 图形化显示 |
| 2 | Ctrl+Alt+F2 | Shell 提示 |
| 3 | Ctrl+Alt+F3 | 安装日志(安装程序的信息) |
| 4 | Ctrl 十 Alt+F4 | 与系统相关的消息 |
| 5 | Ctrl+Alt+F5/F6 | 文本(shell)显示界面 |
| 7 | Ctrl+Alt+F7 | 安装提示对话框 |
| 1 | Ctrl+Alt+F1 | X 图形化显示 |

登录 X WindowSystem 系统后的任何时候，按 Ctrl+Alt+Fn 组合键都可以切换到其他虚拟终端，其中的 Fn 是指 F1 到 F7 功能键。例如，按 Ctrl+Alt+F2 组合键，可切换到第一个虚拟终端；按 Ctrl+Alt+F3 组合键，可切换到第二个虚拟终端；依次类推。若要返回原来的 X WindowSystem 系统界面，可以按 Ctrl+Alt+F1 组合键。

用户也可以在窗口登录界面出现时按 Ctrl+Alt+F7 组合键直接登录文本模式终端。

当然，在 Red Hat Enterprise Linux 7 图形化界面中，通过终端命令程序也可在使用 X WindowSystem 系统的同时使用文本模式。

3. 常用命令

1)　目录操作命令

(1)　查看目录命令 ls

语法：ls [选项] [目录或是文件]

功能：列出目录的内容。该命令类似于 DOS 下的 dir 命令。默认情况下，输出的条目按字母顺序排序。当未给出目录名或是文件名时，就显示当前目录的信息。

(2)　改变工作目录命令 cd

语法：cd [directory]

功能：该命令将当前目录改变至 directory 所指定的目录。利用点点(..)把目录上移一级。

(3)　创建目录命令 mkdir

语法：mkdir [选项] dir-name

功能：创建由 dir-name 命名的目录。该命令类似于 DOS 下的 md 命令。

(4)　删除目录命令 rmdir

语法：rmdir [选项] dir-name

功能：删除目录 dir-name。需要特别注意的是，一个目录被删除之前必须是空的。

(5) 显示当前目录命令 pwd

语法：pwd

功能：此命令显示出当前工作目录的绝对路径。

2) 文件操作命令

(1) 显示文件命令 cat、head、tail、more

① cat 命令

语法：cat [选项] 文件名

功能：在标准输出上显示指定的文件。如果文件内容很长，在一张屏幕显示不下时，会出现屏幕滚动。

② head 命令

语法：head [显示行数] 文件名

功能：在屏幕上显示指定文件最前面的若干行，行数由“显示行数”确定。

③ tail 命令

语法：tail [显示行数] 文件名

功能：在屏幕上显示指定文件末尾的若干行，行数由“显示行数”确定。

语法：tail [+n] 文件名

功能：在屏幕上从指定行号 *n* 开始显示，直到文件的末尾。

④ more 命令

语法：more [选项] 文件名

功能：显示文件内容，每次显示一屏，并在屏幕的底部提示已显示的百分比。按 Space 键显示下一屏的内容，按 Enter 键显示下一行的内容，按 B 键显示上一屏的内容，按 Q 键退出 more 命令。

(2) 创建新文件命令 touch

语法：touch 文件名

功能：创建空文件夹。

(3) 复制文件命令 cp

语法：cp [选项] 源文件或目录 目标文件或目录

功能：把指定的源文件复制到目标文件或把多个源文件复制到目标目录中。该命令同 DOS 下的 copy 命令一样。

(4) 移动和重命名文件命令 mv

语法：mv [选项] 源文件或目录 目标文件或目录

功能：为文件或目录改名或将文件由一个目录移到另一个目录中。当第二个参数类型是文件时，mv 命令完成文件重命名；当第二个参数是已存在的目录名称时，源文件或目录参数可以有多个，mv 命令将各参数指定的源文件均移至目标目录中。

(5) 删除文件命令 rm

语法：rm [选项] 文件

功能：删除不需要的文件和目录。对于链接文件，只是断开了链接，原文件保持不变。

(6) 文件链接命令 ln

语法：ln 源文件 目标文件

功能：在文件间建立链接。如果目标文件是到某一目录文件的目录，源文件会链接到此目录下，文件名不变；如果目标文件不是到某一目录文件的路径，源文件会链接到此目标文件，并覆盖已经存在的同名文件。

(7) 文件内容比较命令 diff 和 cmp

① diff 命令

语法：diff 文件 1 文件 2 …

功能：用于比较文本文件，并显示两个文件的不同。

② cmp 命令

语法：cmp 文件 1 文件 2 …

功能：用于比较数据文件，只报告从哪一个字节开始出现不同。

(8) 查找命令 find 和 locate

① find 命令。

语法：find 路径名 [选项]

功能：查找文件和目录的位置。

② locate 命令。

语法：locate 文件名 [选项]

功能：用于文件和目录的查找。使用 locate 命令的前提是要首先创建一个用于定位文件或目录位置的 slocate 数据库，而且该数据库应是时时更新的，这样才能保证 locate 查找结果的准确性。

(9) 文件中查找正文命令 grep

语法：grep [选项] 查找模式 文件名

功能：在文件中查找指定模式的词或短语，并在标准输出上显示包括给定字符串的所有行。

3) 文件权限操作命令

Linux 系统中的每个文件和目录都有访问许可权限，用来确定谁可以通过何种方式对文件和目录进行访问和操作。

(1) 改变文件属主命令 chmon

语法：chmon [选项] 用户或组文件

功能：更改某个文件或目录的所有权。用户可以是用户名或用户 ID，组可以是组名或组 ID。文件是以空格分开的要改变权限的文件列表、文件参数。

(2) 改变用户组命令 chgrp

语法：chgrp [选项] group 文件名

功能：改变文件或目录所属的组。其中 group 可以是用户组 ID，也可以是/etc/group 文件中用户组的组名。文件名是以空格分开的要改变目录所在的文件列表，支持通配符。如果用户不是该文件的属主或超级用户，则不能改变该文件的组。

(3) chmod

语法：chmod key 文件名

功能：改变文件或目录的访问权限。只有文件主或超级用户 root 才有权用 chmod 命令改变文件或目录的访问权限。

提示：访问权限规定了 3 种不同类型的用户，分别是文件属主(owner)、同组用户(group)和可以访问系统的其他用户(others)。每类用户有 3 种访问方式，即可读(r)、可写(w)、可执行或查找(x)。如图 2-4 所示的文件权限表示，该文件的属主有可读、可写和可执行权力，而同组用户和其他用户只有可读和可执行权力。文件权限也可以由 3 个八进制数来表示，例如，上述文件权限可表示为 755。

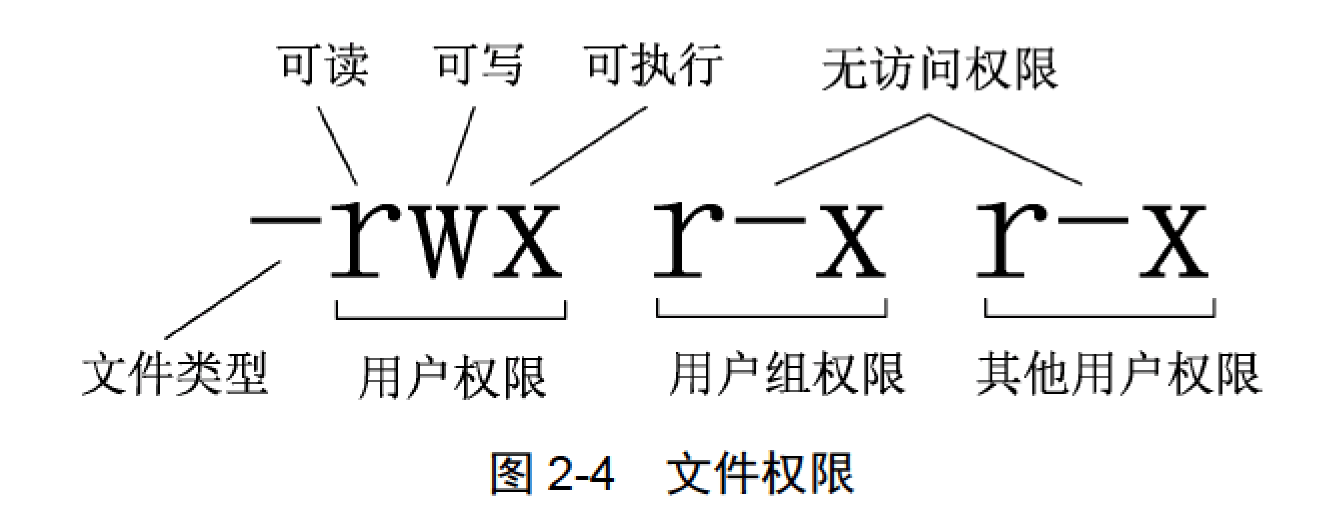



图 2-4　文件权限

4)　进程和作业控制命令

(1)　ps 命令

语法：ps [option [arguments] …]

功能：观察进程状态，把当前瞬间进程的状态显示出来。

(2)　top 命令

功能：用于读入计算机系统的信息，包括当前的系统数据和进程的状态等。

(3)　kill 命令

功能：用于终止进程的执行，释放进程占用的系统资源。

(4)　at 命令

语法：at [选项]　时间[日期]

功能：在指定的时间运行用户安排的作业。

5)　基本网络命令

(1)　telnet　命令

语法：telnet [选项] IP 地址/主机名

功能：用于远程登录。成功连接远程计算机后，telnet 就显示登录信息，提示用户输入注册名和口令。

(2)　ping　命令

语法：ping [选项] IP 地址/主机名

功能：用来确定网络上的主机是否可到达和到达速率。

(3)　inger 命令

语法：inger [选项]　用户@主机名

功能：查询系统用户的信息，显示某个用户的用户名、主目录、停滞时间、登录时间等信息。

## 2.1.2　典型例题分析

**例 1**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2015

年 11 月下午试题二)

【说明】

请根据 Windows 服务器的安装与配置，回答下列问题。

【问题 1】(3 分)

1．下列给出了 Windows 服务器安装步骤，正确的排序为__(1)__。

①选择文件系统格式；②创建分区；③选择授权模式；④设置区域和语言

2．在 Windows 中启动“组策略编辑器”程序，需在“运行”中执行__(2)__。

备选答案：

A. gpedit.com　　B. gpedit.exe　　C. gpedit.msc　　D. gpedit.bat

3．在 Windows 中必须通过安装第三方软件实现的服务是__(3)__。

备选答案：

A. 建立动态网站　　B. 域名解析　　C. 使用 PHP 数据库　　D. 网络打印

【问题 2】(4 分)

请参照图 2-5、图 2-6 所示的网络配置回答问题。

1．图 2-5 配置了两个地址，是为了在一个服务器上实现多个站点的同时访问。这两个 IP 地址__(4)__。

备选答案：

A. 都是真实的地址，可以 ping 通

B. 都是虚拟地址，不可以 ping 通

C. 一个是真实地址，一个是虚拟地址，虚拟地址不可以 ping 通




图 2-5　TCP/IP 配置

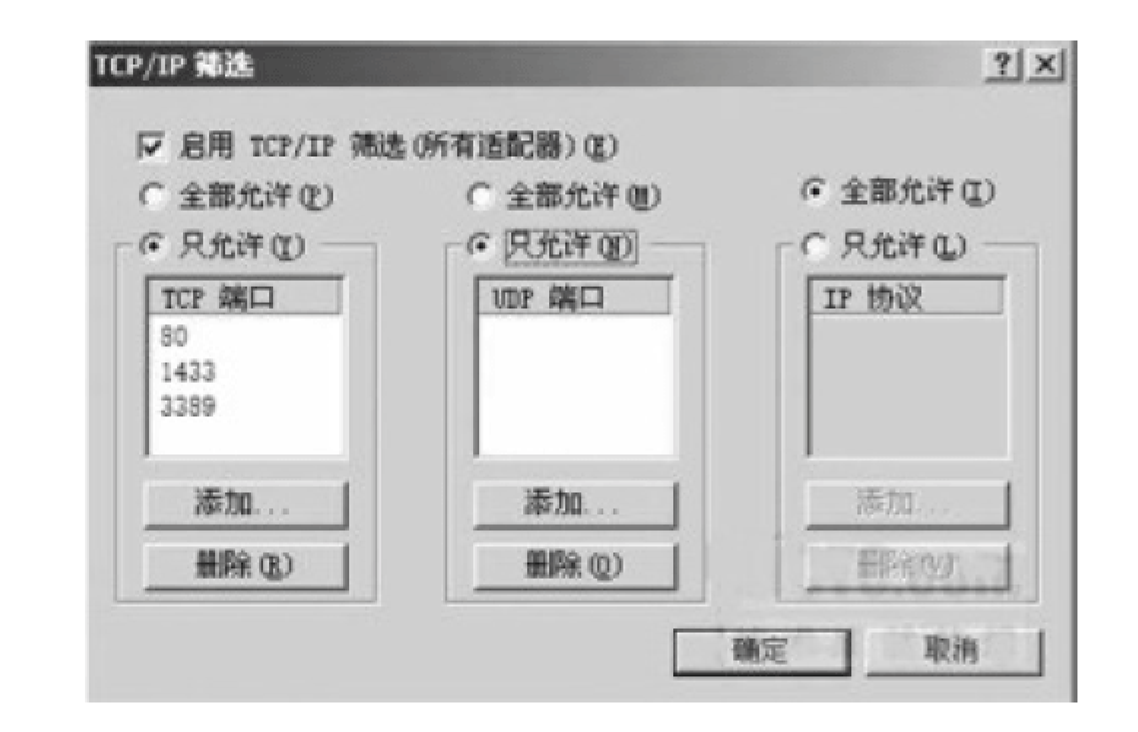



图 2-6　TCP/IP 筛选

2．如图 2-6 所示，开放的 80、1433、3389 这 3 个 TCP 端口分别对应的应用是__(5)__、__(6)__、远程访问。

3．如果如图 2-6 所示，若要将该服务器用作域名解析服务器，应打开 UDP 的__(7)__端口。

备选答案：

A. 53　　B. 23　　C. 443

【问题 3】

请参照图 2-7 所示的用户管理界面，回答下面问题。

1．图 2-7 中“打叉”的用户是因为__(8)__。

备选答案：

A．用户被停用　　B．用户密码过期　　C．没有给用户分配权限

2. 默认情况下，图 2-7 中__(9)__用户权限最高，Internet 来宾账户隶属于__(10)__组。

分析：

【问题 1】

本题考查 Windows 服务器的安装与配置。

此类题目要求考生掌握 Windows 服务器的基本操作命令，了解 Windows 服务器安装的各个环节、参数的设置目的和参数的含义。

创建分区是对服务器硬盘空间进行划分或是对已经划分好的空间进行管理，以便将外部介质中的 Windows 安装程序安装到服务器，接下来的安装步骤需要选择 NTFS 或 FAT 文件系统对分区进行格式化。NTFS 的特点是有效地利用磁盘空间、支持文件级压缩、具备更好的文件安全性。由于 DOS 系统不支持 NTFS，服务器要实现多重引导就需要采用 FAT。




图 2-7　计算机管理窗口

设置区域和语言，目的是配置服务器的放置区域(国别)、输入方法，还包括数字、货币及日期的显示方式等内容。授权模式分为“每服务器”和“每设备或每用户”。“每服务器”模式要求同时连接服务器的每个客户端有单独的“客户访问许可证(CAL)”。该许可证保存在服务器，是软件产品赋予客户端的权利，使其能够访问服务器上的服务。“每设备

或每用户”模式是将访问许可证放在客户端，此种模式适用于多台服务器环境，可以节省开支，减少访问许可证的购买数量。

“组策略编辑器”程序是通过微软管理控制台 MMC(Microsoft Management Console)添加或删除的服务器管理文件，此类文件的扩展名是 msc。

Windows 与 PHP 数据库隶属于不同的软件厂商，在 Windows 环境中使用 PHP 数据需要另外安装。

**【问题 2】**

通过图 2-5 可知，在对 Windows 的配置中可以配置多个 IP 地址对外部提供服务，所配置的 IP 地址都是可用的，可以进行 ping 测试。

在网络技术中，端口(Port)分为两种。一种是物理意义上的端口，如 ADSLModem、集线器、交换机、路由器用于连接其他网络设备的接口，像 RJ-45 端口、SC 端口等。另一种是逻辑意义上的端口，端口号的范围从 0～65535，比如用于浏览网页服务的 80 端口、用于 FTP 服务的 21 端口等。

TCP 是指传输控制协议，提供的是面向连接、可靠的字节流服务。UDP 是指用户数据报协议，是一个简单的面向数据报的运输层协议。UDP 不提供可靠性，它只是把应用程序传给 IP 层的数据报发送出去，但是并不能保证它们能到达目的地。

**【问题 3】**

对 Windows 用户的管理是通过 Windows 中的“计算机管理”界面来实现的，通过单击图 2-7 中的“用户”实现用户的添加、删除、重命名、修改密码、更改密码等操作。当某个用户被停用时，显示的用户名就会被标记为“打叉”状态。

Administrator 属于 Administrators 本地组内的用户，具备系统管理员的权限，有最大的控制权限。Windows 除了 Administrators 组，还设置多个不同权限的组，比如：Users 普通用户组，分配给该组的默认权限不允许成员修改操作系统的设置或用户资料，Users 组提供了一个最安全的程序运行环境。Guests 来宾组，来宾组跟普通组 Users 的成员有同等访问权，主要用于远程登录。

**答案：**

**【问题 1】**

(1) 2-1-4-3　　(2) C　　(3) C

**【问题 2】**

(4) A　　(5) Web　　(6) SQL　　(7) A

**【问题 3】**

(8) A　　(9) Administrator　　(10) User

## 2.1.3　同步练习

阅读以下关于 Linux 网卡安装和配置过程的说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。

**【说明】**

某个采用动态 IP 地址分配策略的计算机使用了最新的 BCM 5751 网卡芯片，由于 Red

Hat Linux 9 操作系统无法自动识别此硬件，需要单独安装驱动程序才能正常工作。安装过程如下。

(1) 将驱动程序压缩文件 bcm5700-8.3.14.tar.gz 复制到一个临时目录中，并使用解压缩命令将驱动程序包 bcm5700-8.3.14.tar.gz 解压缩。

(2) 用 make 命令构建驱动程序的可加载模块。

(3) 用 make install 命令加载驱动程序。

(4) 重新启动系统，启动过程中系统找到网卡进行相应参数配置。

**【问题 1】**(2 分)

将文件 bcm5700-8.3.14.tar.gz 解压缩的命令是__(1)__。

A. rar　　B. tar　　C. unzip　　D. rpm

**【问题 2】**(3 分)

打开/etc/sysconfig/network 文件，内容如下：

```
NETWORKING=__(2)__
HOSTNAME=localhost.localdomain
```

打开并编辑网络接口文件/etc/sysconfig/network-scripts/ifcfg-eth0，内容如下：

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=__(3)__
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

从备选答案中为(2)和(3)空缺处选择恰当内容，填入答题纸对应的解答栏内。

A. yes　　B. no　　C. dhcp　　D. auto

**【问题 3】**(3 分)

在/etc/sysconfig/network-scripts/目录中有许多脚本命令，运行该目录下的__(4)__命令，可以启动该网卡，该命令的命令行参数是__(5)__(填空)。

(4)的备选答案是：

A. ifdown　　B. ifup　　C. netdown　　D. netup

**【问题 4】**(5 分)

可以使用程序__(6)__来查看网络接口的运行情况，输出如下：

```
eth0 Link encap:Ethernet  Hwaddr:00:12:3F:94:E7:B9
inet addr:192.168.0.63  Bcast:__(7)__Mast:__(8)__
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:1501  errors:0  dropped:0  overruns:0  frame:0
TX packets:74  errors:0  dropped:0  overruns:0  carrier:0
collisions:0  txqueuelen:100
RX bytes:164444 (160.5 Kb)  TX bytes:9167 (8.9 Kb)
Interrupt:11  Memory:dfcf0000-dfd00000
```

上述输出表明，该网卡运行__(9)__(填“正常”或“不正常”)；上文中 MTU 的含义是__(10)__。

**【问题 5】**(2 分)

运行 route-n 命令，可以输出路由选择表如下：

```
Kernel  IP  routing  table
Destination  Gateway      Genmask         Flags  Metric  Ref  Use  Iface
192.168.0.0  0.0.0.0     255.255.255.0     U       0       0    0    eth0
169.254.0.0  0.0.0.0     255.255.0.0       U       0       0    0    eth0
127.0.0.0    0.0.0.0     255.0.0.0         U       0       0    0    lo
0.0.0.0    192.168.0.1   0.0.0.0           UG      0       0    0    eth0
```

则该网络的默认网关地址是 (11) 。

## 2.1.4　同步练习参考答案

**【问题 1】**

(1) B

**【问题 2】**

(2) A　　　　(3) C

**【问题 3】**

(4) B　　　　(5) eth0

**【问题 4】**

(6) ifconfig

(7) 192.168.0.255

(8) 255.255.255.0

(9) 正常

(10) 最大传输单元

**【问题 5】**

(11) 192.168.0.1

# 2.2　DNS 服务器配置

## 2.2.1　考点辅导

### 2.2.1.1　Windows Server 2008 R2 DNS 服务器的安装与配置

1. 安装 DNS 服务

Windows Server 2008 R2 系统内置了 DNS 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供域名解析服务。

在一台运行 Windows Server 2008 R2 的计算机上安装 DNS 服务器的操作步骤如下。

(1) 选择“开始”→“管理工具”→“服务器管理器”→“角色”命令，在打开的窗

口中单击“添加角色”按钮，启动 Windows 添加角色向导。

(2) 在“服务器角色”列表框中选中“DNS 服务器”复选框，并单击“下一步”按钮。按照向导提示，执行至确认界面，单击“安装”完成 DNS 服务器的安装。

2. 设置 DNS 服务器

安装完 DNS 服务器后，需要对其进行设置，这样 DNS 服务器才能为客户机提供服务。用于配置和管理 Windows Server 2008 R2 DNS 服务器的主要工具是 DNS 控制台 dnsmgmt。

从“管理工具”窗口中单击 DNS，可以看出 DNS 控制台已默认将本地服务器列在控制台左侧的树中。

假设局域网的域名为 example.com，其中有一台主机作为 WWW 服务器，IP 地址为 192.168.1.30，按照惯例将这台主机命名为 www.example.com。下面介绍如何在 DNS 服务器中实现对该主机名称的解析，步骤如下。

(1) 首先在 DNS 服务器中新建一个名为 example.com 的区域。右击控制台目录树中的 EX-WIN2008SVR 服务器，在弹出的快捷菜单中选择“配置 DNS 服务器”命令，打开“配置 DNS 服务器向导”对话框，单击“下一步”按钮。

(2) 在“选择配置操作”对话框中，为了讲解 DNS 服务器的配置，选择“创建正向和反向查找区域”，单击“下一步”按钮。

**提示：** 正向查找区域用于进行 DNS 正向查询，即允许客户端通过已知的主机名，查找其所对应的 IP 地址；反向查找区域用于进行 DNS 反向查询，即允许客户端使用已知的 IP 地址，查找其所对应的计算机名。

(3) 在“新建区域向导”对话框中，由于此时配置的是网络内的第一台 DNS 服务器，所以选中创建“主要区域”单选按钮，单击“下一步”按钮。

(4) 在“区域名称”文本框中输入区域的名称 example.com，如图 2-8 所示，单击“下一步”按钮。

(5) 在“区域文件”对话框中，选中“创建新文件，文件名为”单选按钮，并使用系统默认的文件名 example.com.dns，单击“下一步”按钮，如图 2-9 所示。

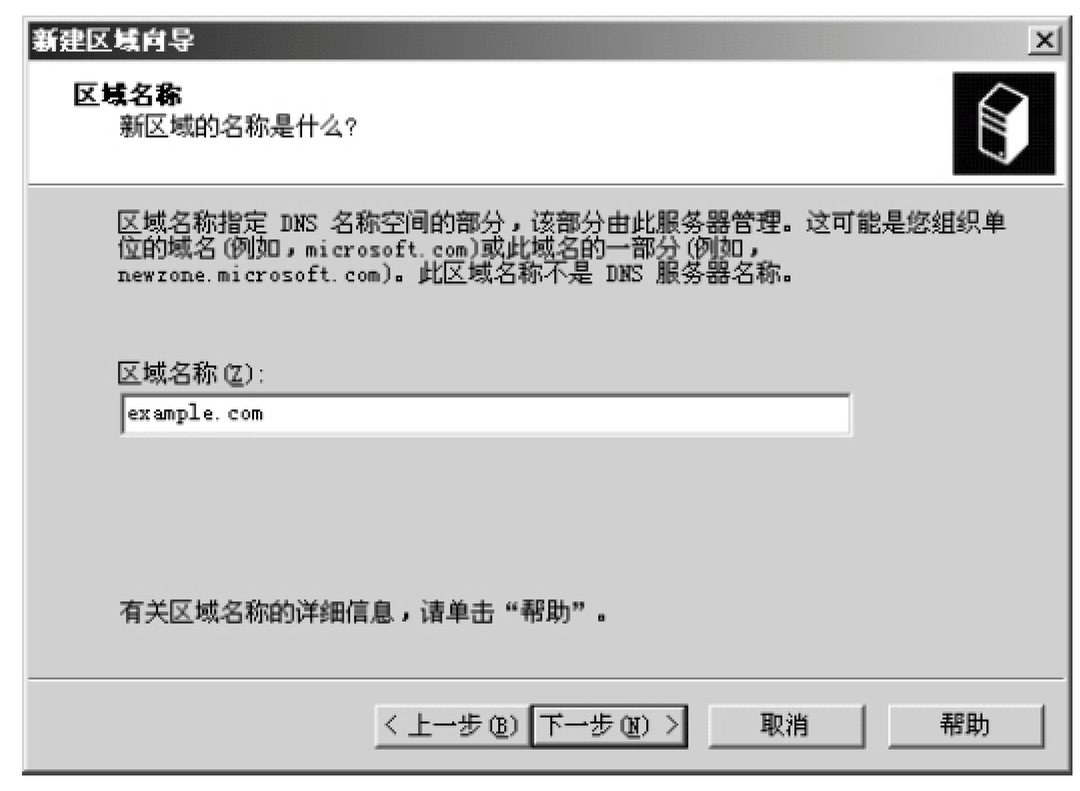



图 2-8 输入区域名称

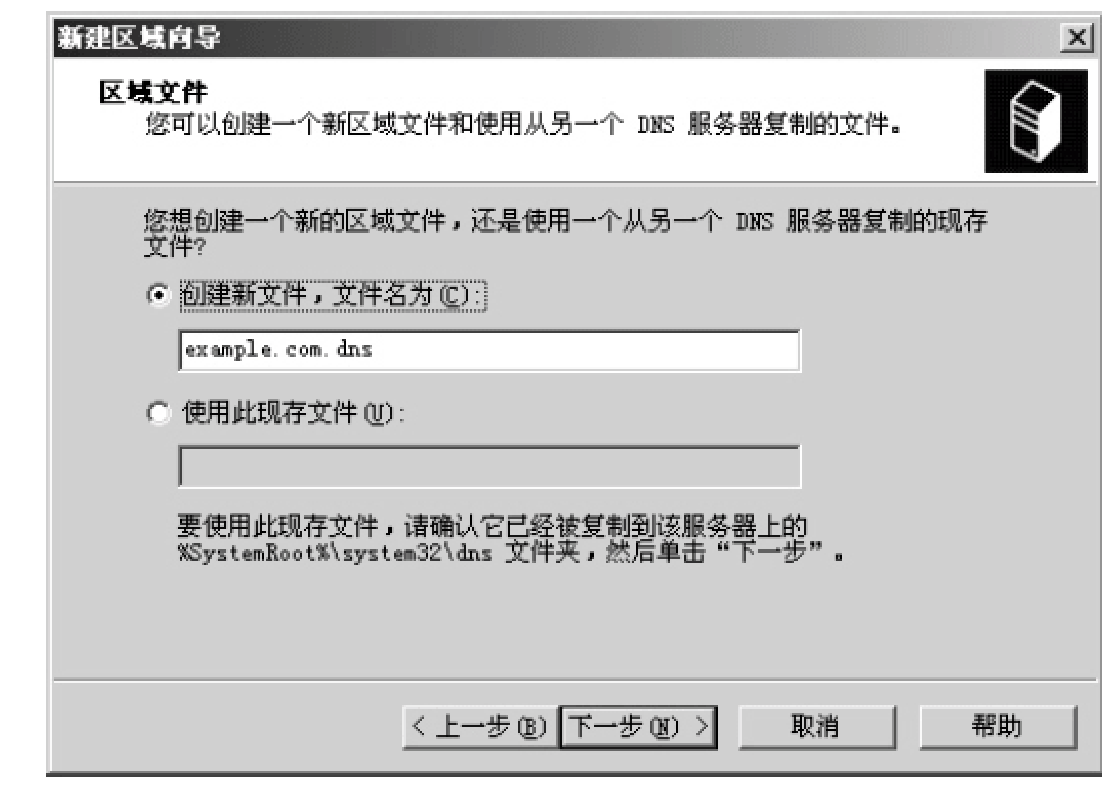



图 2-9 创建新的区域文件

(6) 在“动态更新”对话框中，选中“不允许动态更新”单选按钮，如果服务器已安

装了 Active Directory，也可以选中“只允许安全的动态更新”单选按钮，以便最大限度地集成和支持 Active Directory 以及增强的 DNS 服务器功能。单击“下一步”按钮，如图 2-10 所示。

(7) 接下来配置反向区域，在“反向查找区域”对话框中，选中“是，现在创建反向查找区域”单选按钮，单击“下一步”按钮。在接下来的“区域类型”对话框中，依旧选中“主要区域”单选按钮，再单击“下一步”按钮。

(8) 在“反向查找区域名称”对话框中，选中“网络 ID”单选按钮，并在下面输入本网络的网络 ID，如 192.168.1，如图 2-11 所示，单击“下一步”按钮。

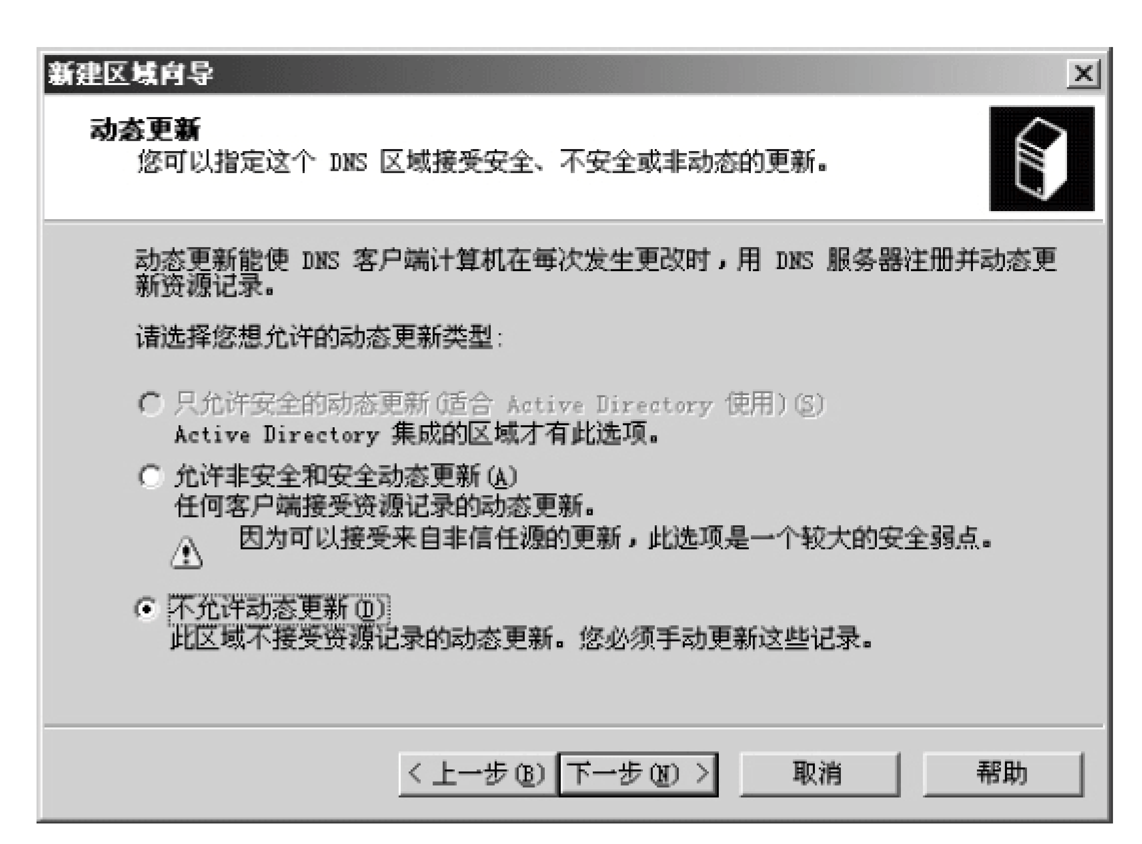


图 2-10　设置 DNS 服务器动态更新类型

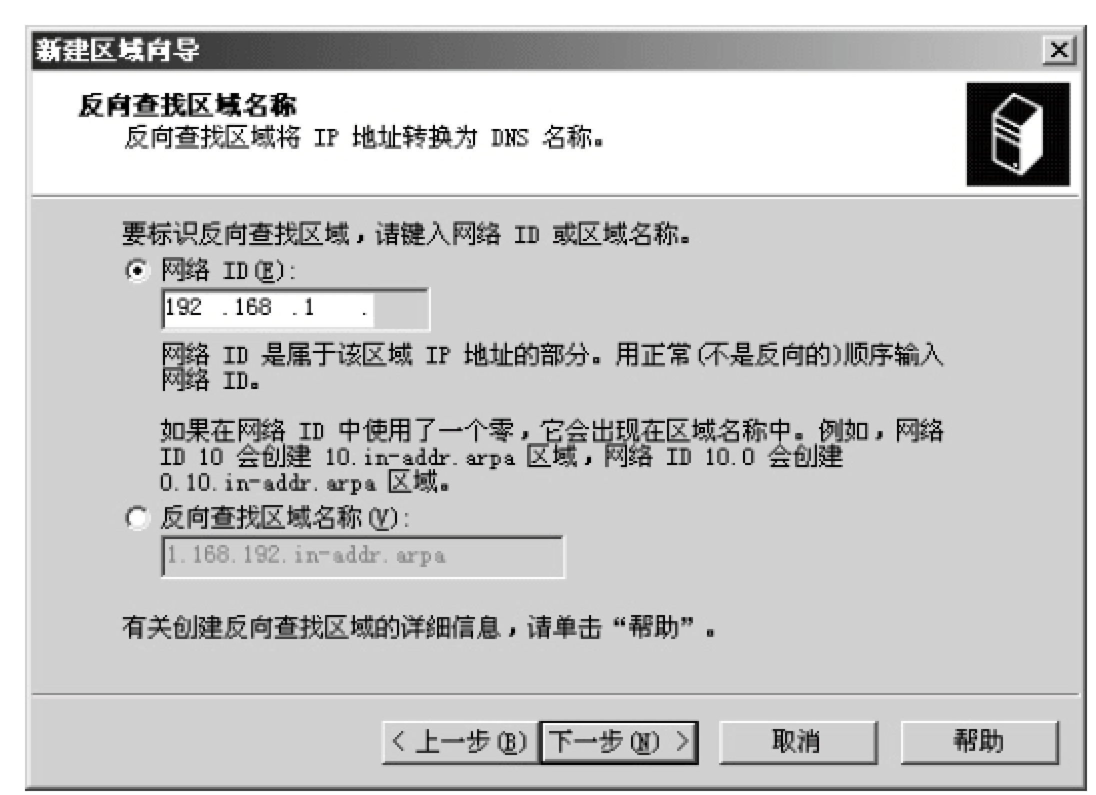


图 2-11　设置反向查找区域名称

(9) 在接下来的“区域文件”和“动态更新”两个对话框中，分别选中“创建新文件，文件名为”和“不允许动态更新”单选按钮，文件名按照系统默认给出。

(10) 在“转发器”对话框中，暂时选中“否，不向前转发查询”单选按钮。转发器的具体用途和配置方法后面会做进一步介绍。单击“下一步”按钮，如果配置顺利，会弹出一个对话框，提示已成功地完成了 DNS 服务器配置向导，单击“确定”按钮关闭对话框。

DNS 服务器配置完成后，在控制台的目录树中可以看到，服务器节点下建立了“正向查找区域”和“反向查找区域”。双击展开“正向查找区域”，会看到新区域 example.com 已经添加。单击 example.com，右半窗口中会显示该区域的配置信息。

### 3. 创建域名

下面介绍如何建立主机 www.example.com，其操作步骤如下。

(1) 依次执行“开始”→“管理工具”→DNS 命令，打开 dnsmgmt 控制台窗口。

(2) 在左窗格中依次展开 ServerName→“正向查找区域”目录，然后用鼠标右击区域名处，从弹出的快捷菜单中选择“新建主机”命令，弹出如图 2-12 所示的对话框，输入主机名 www，IP 地址 192.168.1.30。

(3) 如果希望 DNS 服务器也能够进行反向查询，则选中“创建相关的指针(PTR)记录”复选框，单击“添加主机”按钮。如果添加成功，系统会提示：“成功地创建了主机记录 example.com。”如图 2-13 所示，单击“确定”按钮。

(4) 如果不再添加主机，单击“完成”按钮。

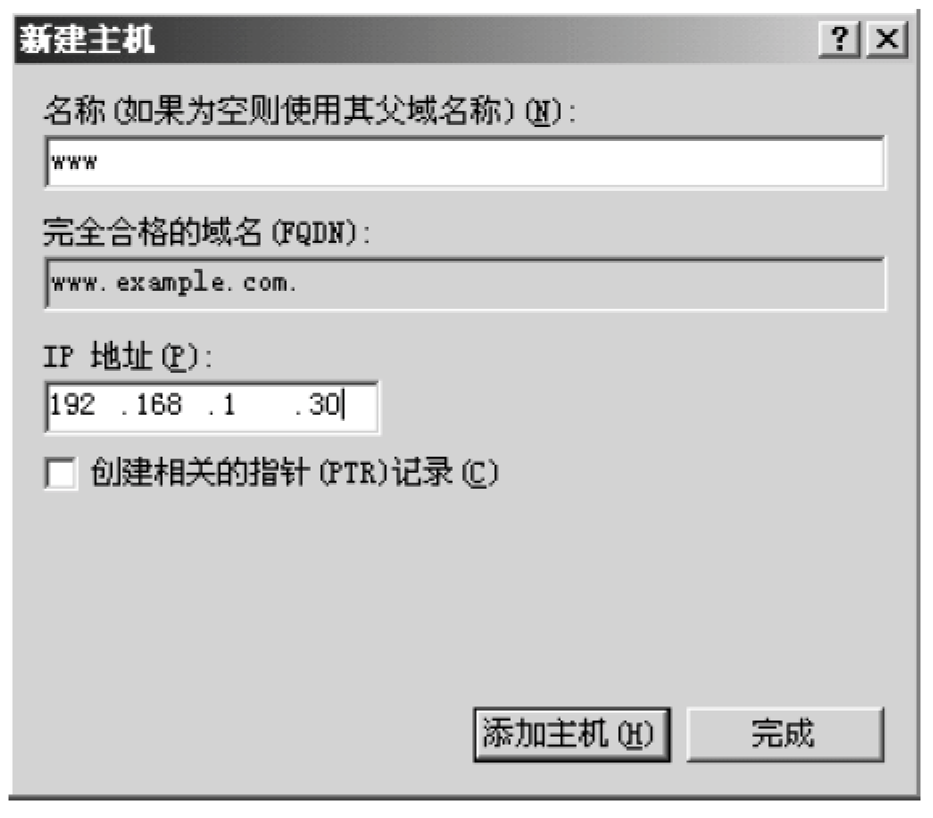



图 2-12 “新建主机”对话框




图 2-13 主机记录创建成功

4. 安装客户端

安装 DNS 客户机的步骤如下。

(1) 在“控制面板”对话框中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右键单击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，在打开的“本地连接 属性”对话框中选中“Internet 协议(TCP/IP)”复选框，单击“属性”按钮，打开如图 2-14 所示的对话框。

(4) 在图 2-14 的“首选 DNS 服务器”文本框中输入一台 DNS 服务器的 IP 地址，然后单击“确定”按钮，这样便把该计算机配置为那台 DNS 服务器的 DNS 客户机了。




图 2-14 “Internet 协议(TCP/IP)属性”对话框

### 2.2.1.2　Red Flag Server 下 DNS 服务器的安装与配置

1. 打开 DNS 配置工具

打开 DNS 配置工具，必须在 KDE 环境下以 root 权限来运行 DNS 配置工具 rfdns。其启动方法有以下 3 种。

(1) 在系统主菜单中选择“系统”→“控制面板”命令，打开“控制面板”窗口，在“网络服务配置”选项卡中双击“DNS 配置工具”选项。

(2) 在系统主菜单中选择“管理工具”→“DNS 配置工具”命令。

(3) 在运行命令或 Shell 提示符下直接输入 rfdns。

2. 启动和停止 DNS 服务

启动、停止和重新启动 DNS 服务可以通过 DNS 配置工具 rfdns 来进行，也可以通过命令行终端来完成。

(1) 通过 DNS 配置工具 rfdns 来启动、停止和重新启动 DNS 服务的步骤如下。

① 启动 DNS 配置工具 rfdns。

② 在控制台菜单中选择“操作”→“所有任务”命令，然后选择“启动”命令可以启动 DNS 服务，选择“停止”命令可以停止 DNS 服务，选择“重新启动”命令可以重新启动 DNS 服务。

(2) 通过命令行终端来启动、停止和重新启动 DNS 服务的命令如下。

- 启动 DNS 服务：#/etc/init.d/named start。
- 停止 DNS 服务：#/etc/init.d/named stop。
- 重新启动 DNS 服务：#/etc/init.d/named restart。

3. 在 Red Flag Server 中添加正向查找区域

(1) 添加正向标准主要区域的步骤如下。

① 在配置工具主窗口左侧的控制台树中，右击“正向查找区域”选项。在弹出的快捷菜单中选择“操作”→“新建区域”命令，弹出“新建区域向导”对话框，单击“下一步”按钮继续。

② 在出现的“区域类型”界面中，建立一个全新的区域。选中“主要区域”单选按钮，单击“下一步”按钮继续。

③ 在出现的“区域名称”界面中输入新建区域的名称。如果申请的是一组域名，如 abc.com，则只要输入到二级域，而不是连同子域或主机名称一起输入，单击“下一步”按钮继续。

④ 在出现的“区域文件”界面中，如果要创建一个新的区域文件，就直接使用提示的文件名来添加数据。如果这个区域要使用从另一台计算机上复制的文件，可选中“使用此现存文件”单选按钮。选择区域文件后单击“下一步”按钮继续。

⑤ 在出现的“正在完成新建区域向导”界面中，将显示以上步骤所设置的数据列表。如果一切设置正确，单击“完成”按钮将建立一个正向查找区域。新建的区域将添加到主窗口的控制台树中。

(2) 添加正向标准辅助区域的步骤如下。

① 添加正向标准辅助区域与添加正向标准主要区域的步骤相同，在“区域类型”界面中选中“辅助区域”单选按钮，单击“下一步”按钮继续。

② 在“区域名称”界面中为新添加的区域命名后，单击“下一步”按钮进入“设置复制区域”界面，设置想要复制区域的服务器。此步骤用来设置想要复制区域的 DNS 服务器源，可以一次复制多个服务器的数据。

③ 在“IP 地址”中输入可复制的服务器 IP 地址后单击“添加”按钮；也可以在“服务器名”文本框中输入服务器的主机名后，单击“解析”按钮获得其 IP 地址再添加。

④ 单击“下一步”按钮，然后依向导提示完成设置。新建的区域将添加到主窗口的控制台树中。

4. *在 Red Flag Server 中添加反向查找区域*

这里仅介绍添加反向标准主要区域的过程。添加反向标准辅助区域的过程与添加正向标准辅助区域的过程基本相同，这里就不再介绍了。添加反向标准主要区域的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，右击“反向查找区域”选项。在弹出的快捷菜单中选择“操作”→“新建区域”命令，弹出“新建区域向导”对话框，单击“下一步”按钮继续。

(2) 在出现的“区域类型”对话框中，开始建立一个全新的区域，选中“主要区域”单选按钮，单击“下一步”按钮继续。

(3) 在出现的“反向查找区域”界面的“网络 ID”文本中，应该以 DNS 服务器 IP 地址的前三段来设置反向查找区域。例如，使用 DNS 服务器的 IP 地址是 172.16.82.11，则取其前三段，即 172.16.82。然后系统会在“反向查找区域名称”文本框中自动设置为 82.16.172.in-addr.arpa，单击“下一步”按钮继续。

(4) 在出现的“区域文件”界面中，直接使用默认的文件名即可，单击“下一步”按钮继续。

(5) 在出现的“正在完成新建区域向导”界面中，将显示以上步骤所设置的数据列表。如果一切设置正确，单击“完成”按钮将建立一个反向查找区域。新建的区域将添加到主窗口的控制台树中。

5. *在 Red Flag Server 中配置区域属性*

1) 修改区域的起始授权机构(SOA)记录

SOA(Start Of Authority)用来识别域名中由哪一个名称服务器负责信息授权，在区域数据库文件中，第一条记录必须是 SOA 的设置记录。

在配置工具主窗口左侧的控制台树中，选中相应的区域。选择菜单中的“操作”→“属性”命令，或右击选择快捷菜单中的“属性”命令，打开“区域属性”对话框，切换到“起始授权机构(SOA)”选项卡。

如有需要，可以修改起始授权机构(SOA)的属性。要调整“刷新间隔”“重试间隔”或“过期间隔”，在下拉列表框中选择以秒、分钟、小时、天或星期为单位的时间段，然后在文本框中输入数字。单击“应用”按钮，保存调整后的间隔。完成更改后单击“确定”按钮使修改生效。

2) 将其他 DNS 服务器指定为区域的权威服务器

在配置工具主窗口左侧的控制台树中选择相应的区域，选择菜单中的“操作”→“属

性”命令，或右击选择快捷菜单中的“属性”命令，打开“区域属性”对话框，切换到“名称服务器”选项卡。

如果要向列表中添加名称服务器，单击“添加”按钮即可弹出“新建名称服务器”对话框。按 IP 地址指定其他的 DNS 服务器，然后单击“添加”按钮将它们加入列表。也可以通过指定服务器 IP 地址或输入其 DNS 名称将区域添加到权威服务器的列表中。输入名称时，单击“解析”按钮可以在将它添加到列表之前将其名称解析为 IP 地址。

使用该过程指定的 DNS 服务器将被加入到该区域的现有名称服务器(NS)资源记录中。

3)　为辅助区域更新主控服务器

在配置工具主窗口左侧的控制台树中，选择相应的辅助区域。选择菜单中的“操作”→“属性”命令，也可以右击选择快捷菜单中的“属性”命令，打开“区域属性”对话框。

切换到“常规”选项卡，在“IP 地址”中为新的主控服务器指定 IP 地址并单击“添加”按钮以便在列表中更新。

#### 6. 管理资源记录

1)　添加主机资源记录

向区域中添加主机资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择相应的正向查找区域。选择菜单中的“操作”→“新建主机”命令，或右击选择快捷菜单中的“新建主机”命令，打开“新建主机”对话框。

(2) 在“名称”文本框中，输入新增主机记录的名称。不需要输入整个域名，比如要新增 sales 名称，只需输入 sales，而不是 sales.abc.com。

(3) 在“IP 地址”文本框中，输入新建主机的实际 IP 地址。

(4) 单击“添加主机”按钮，新增的主机记录将显示在主窗口右侧的列表中。重复上述操作可以向区域中添加多个主机资源记录。

2)　添加别名(CNAME)的资源记录

设置别名可以让一个主机拥有多个主机名称。例如，当一个主机作为 Web 服务器时为 www.abc.com，而当作为 FTP 服务器时可以是 ftp.abc.com。向区域添加别名(CNAME)的资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择相应的正向查找区域。选择菜单中的“操作”→“新建别名”命令，或右击选择快捷菜单中的“新建别名”命令，打开“新建资源记录”对话框。

(2) 在“别名”文本框中输入别名，在“目标主机的完全合格的域名”文本框中输入使用此别名的 DNS 主机的完全合格域名。

(3) 单击“确定”按钮完成新增主机别名的操作。新增的主机别名将出现在主窗口右侧的列表中。

3)　添加邮件交换器资源记录

向区域添加邮件交换器(MX)资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择相应的正向查找区域。选择菜单中的“操作”→“新建邮件交换器”命令，或右击选择快捷菜单中的“新建邮件交换器”命令，

打开“新建资源记录”对话框。

(2) 切换到“邮件交换器”选项卡。在“主机或子域”文本框中输入使用此记录发送邮件的服务器域名。在“邮件服务器的完全合格的域名”文本框中输入邮件交换器或邮件服务器主机(发送指定域名的邮件)的 DNS 主机名。

(3) 若该区域内有多台同样域名的邮件服务器，可以调整此区域的“邮件服务器优先级”，数字较小的优先级较高。

(4) 单击“确定”按钮完成新增邮件交换器的操作。新增的邮件交换器记录将显示在主窗口右侧的列表中。

4) 添加指针(PTR)资源记录

向反向查找区域添加指针(PTR)资源记录的步骤如下。

(1) 在配置工具主窗口左侧的控制台树中，选择适当的反向查找区域。选择菜单中的“操作”→“新建指针”命令，或右击选择快捷菜单中的“新建指针”命令，弹出“新建资源记录”对话框。

(2) 在“主机 IP 号”文本框中输入主机 IP 地址的 8 位字节数。在“主机名”文本框中输入 DNS 主机的完全合格域名，该计算机使用此指针记录提供反向搜索(把 IP 地址解析为域名)。

(3) 单击“确定”按钮建立新增的指针。新增的指针记录将显示在主窗口右侧的列表中。

5) 修改区域中的现有资源记录

在配置工具主窗口左侧的控制台树中，单击相应的区域，窗口右侧会显示该区域的详细信息列表。选择要修改的资源记录项，选择菜单中的“操作”→“属性”命令，或右击选择快捷菜单中的“属性”命令，打开“区域属性”对话框，在相应的属性对话框中可以根据需要查看或编辑任何可以修改的属性。

6) 从区域中删除资源记录

在配置工具主窗口左侧的控制台树中，单击相应的区域，窗口右侧会显示该区域的详细信息列表。选中要删除的资源记录项，选择菜单中的“操作”→“删除”命令，或右击该项并在快捷菜单中选择“删除”命令。当出现提示对话框时，确认是否删除所选的资源记录即可。

7) 使用 rfdns 编辑器

为了使用户能够全面地配置 DNS 服务器支持的全部功能，rfdns 配置工具中提供了一个配置文件编辑器。用户可以通过它直接对 DNS 配置文件进行手工修改(后面将要详细介绍)。在菜单中选择“查看”→“编辑器”命令，可以切换文件编辑窗口的隐藏与显示。

选中某一区域或资源记录，其对应的配置内容会在配置文件编辑器中被高亮显示出来。对相应配置文件进行编辑后，单击工具栏中的“存储配置文件”按钮。

配置工具也可以检查配置文件的语法错误，检查结果会显示在消息窗口中。如果出现语法错误，应根据提示进行修改。在开始手工修改配置文件后，不要在存储之前使用配置工具提供的其他配置功能；否则所作的修改将会被覆盖。配置文件修改并存储后，必须重新启动 DNS 服务器才能使修改生效。

### 2.2.1.3　Linux 操作系统下的 DNS 客户端配置文件

每台 Linux 主机要实现域名解析(不管它是不是域名服务器)都需要配置 DNS 客户端配置文件。Linux 操作系统下的 DNS 客户端配置文件主要有两个：一个是名称转换控制文件，另一个是域名转换程序配置文件。

1. *名称转换控制文件*

不同的 Linux 中使用不同的名称转换控制文件，在 Red Flag Linux 中使用/etc/nsswitch.conf 文件，而在 Red Hat Linux 中使用/etc/host.conf 文件。

在 Red Flag Linux 中，/etc/nsswitch.conf 文件用于存放本地主机名以及经常访问 IP 地址的主机名。和域名服务有关的一项是 hosts。在对 IP 进行域名解析时可以设定为先访问该文件，再访问 DNS，最后访问 NIS。这一行文件内容如下：

```
hosts: files dns nisplus nis
```

在 Red Hat Linux 中，/etc/host.conf 文件是用来控制转换程序的设置文件。该文件告诉转换程序使用哪些服务及按照什么顺序进行。可以通过 order 来指定，这一行文件内容如下：

```
order hosts,dns,nis
```

在 Red Hat Linux 中，使用/etc/hosts 文件来存放本地主机名以及经常访问 IP 地址的主机名。

2. *域名转换程序配置文件*

该配置文件是/etc/resolv.conf，它用来设置主机所在域名、域名查找的顺序以及域名服务器的 IP 地址。下面是一个域名转换程序配置文件的例子：

```
domain abc.com.cn
search abc.com.cn xyz.com.cn
nameserver 10.1.14.61
nameserver 10.1.14.62
```

【说明】

- domain 用来定义主机的本地域名。
- search 用来设置查找域名表。如果要查询的只有主机名称，而不含完整的域名时，会加上这里的域名去查找。如果没设置，就会自动加上 domain 设置的域名。
- nameserver 列出域名服务器的 IP 地址。可以设置多个域名服务器，若第一个不能提供服务时就会自动使用第二个。如果 Linux 主机本身就是一台域名服务器，为提高查询速度，应把第一个 nameserver 设置为本地环回地址 127.0.0.1。

### 2.2.1.4　Linux 操作系统下的 DNS 服务器配置文件

在 Linux 操作系统下，有一些和 DNS 服务器配置密切相关的文件，这里做一下简要介绍。下面以一个组织的主域名服务器配置为例。该组织的域名为 abc.com.cn，所使用的网络地址为 210.45.12.0，共有两台服务器：一台的 IP 地址是 210.45.12.100，名字是 a100，它用作域名服务、电子邮件服务；另一台的 IP 地址是 210.45.12.101，名字是 a101，它用作 Web 服务。

1. DNS 服务主配置文件/etc/named.conf

该文件是域名服务器守护进程 named 启动时读取到内存的第一个文件。在该文件中定义了域名服务器的类型、所授权管理的域以及相应数据库文件和其所在的目录。该文件默认的名字是/etc/named.conf。

named.conf 文件的配置一般包括一个全局配置选项(options)部分和多个区(zone)声明部分。

1) 全局配置选项 options

最常用的全局配置选项是定义服务器配置文件的工作目录和转发服务器的 IP 地址。例如：

```
options {
directory "/var/named";
forwarders{
    202.96.134.133;
        };
};
```

【说明】

- directory 指定了 DNS 数据文件的存放目录是/var/named。
- forwarders {202.96.134.133;}，其中 202.96.134.133 是转发 DNS 服务器的地址，forwarders 参数指定其后的 IP 所在的服务器作为备选的 DNS 服务器。也就是说，把本机 DNS 不能解析的主机发送到这个备选的 DNS 服务器上，让它来进行解析。

2) 区声明

区声明是配置文件中最重要的部分，可有多个区声明，每一条区声明需要说明域名、服务器的类型和域信息源 3 项。例如：

```
zone "abc.com.cn" IN {
type master;
file " named.hosts";
notify no;
};
```

【说明】

- zone “abc.com.cn”用于定义这个区的名称。
- type 指定服务器类型。可选的类型有 master、slave 和 hint。master 说明一个区的主域名服务器；slave 说明一个区的辅助域名服务器；hint 说明一个区的高速缓存文件。可以通过该参数来说明这台服务器是主域名服务器、辅助域名服务器还是缓存域名服务器。
- file 指明该区资源记录存放的文件名称。
- notify 用来设置是否自动发出 DNS NOTIFY 信息，其预设值为 yes，也就是当主域名服务器中数据库文件发生修改时，自动发出 DNS NOTIFY 信息，当辅助域名服务器收到这个信息后就自动向主域名服务器确认是否需要更新资料，并自动更新。

(1) 根域名区声明。

该区用来告诉域名服务器的守护程序必须维护一个高速缓存域名服务器，同时还告诉域名服务器的守护程序利用什么文件去初始化高速缓存，其类型必须设置为 hint，该文件一般存放在 named.ca 中。例如：

```
zone "." IN {
type hint;
file "named.ca";
};
```

(2) 反向环回地址区声明。

反向环回地址区主要用于设置环回地址反向解析文件的位置。其内容如下：

```
zone "0.0.127.in-addr.arpa" IN {
type master;
file "named.local";
allow-update { none; };
};
```

(3) 正向域名解析区声明。

正向域名解析区主要用来设置本区域正向域名解析数据文件。若该 DNS 服务器是一个缓存域名服务器，则不需要配置该区；若该 DNS 服务器是一个主域名服务器，则 type 指定为 master。下面的例子是一个主域名服务器，其域名为 abc.com.cn，正向域名解析数据存放在 named.hosts 文件之中：

```
zone " abc.com.cn " IN {
type master;
file " named.hosts";
allow-update { none; };
};
```

如果是辅助域名服务器，则 type 指定为 slave，同时还要指定主域名服务器的 IP 地址，以便进行数据库更新。其格式为 masters{<主域名服务器的 IP 地址>}。例如，主域名服务器地址为 210.45.12.101，则其内容如下：

```
zone " abc.com.cn " IN {
type slave;
file "named.hosts";
masters{210.45.12.101}
};
```

(4) 反向域名解析区声明。

反向域名解析区主要用来设置本区域反向域名解析数据文件。若该 DNS 服务器是一个缓存域名服务器，也不需要配置该区；若该 DNS 服务器是一个主域名服务器，则 type 指定为 master。下面的例子是一个主域名服务器，它负责 210.45.12.0 网络的反向解析，反向域名解析数据存放在 named.rev 文件中。

```
zone "12.45.210.in-addr.arpa" IN {
type master;
```

```
file "named.rev";
allow-update { none; };
};
```

如果是辅助域名服务器，则 type 指定为 slave，同时还要指定主域名服务器的 IP 地址，以便进行数据库更新。其格式为 masters{<主域名服务器的 IP 地址>}。例如，主域名服务器地址为 210.45.12.101，则内容如下：

```
zone "12.45.210.in-addr.arpa" IN {
type slave;
file "named.rev";
masters{210.45.12.101}
};
```

2. DNS 的数据库文件和资源记录

1) 资源记录

在/etc/named.conf 文件中所定义的文件都是 DNS 数据库文件(如本例中 named.ca、named.local、named.hosts、named.rev)，每个文件都由资源记录构成。每条资源记录包含与特定主机的有关信息。而每一条资源记录通常包含 5 项，排成一行记录在文本文件之中，其格式如下：

```
[域名] [存活期 ttl] IN <记录类型> <记录数据>
```

- 域名：给出要定义的资源的域名，该域名通常用来作为域名查询时的关键字。
- 存活期：在存活期内该记录有效；存活期过后该记录不再有效。
- IN：将记录标识为一个 Internet DNS 资源记录。
- 记录类型：该项表明资源记录的类型(下面将详细介绍)。
- 记录数据：说明和该资源记录相关的信息，通常由资源记录类型来决定。

资源记录主要有以下几种类型。

- 主机(A)记录。用来记录在正向查找区域内的主机及其 IP 地址。用户可通过该类型的资源记录把主机域名映射为 IP 地址。
- 主机别名(CNAME)记录。在某些情况下，需要为区域内的一台主机创建多个主机名称。例如，一台主机同时是 Web 服务器与 FTP 服务器，则可以为该主机取两个不同的名称，当作为 Web 服务器时域名是 www.abc.com，而当作为 FTP 服务器时域名可以是 ftp.abc.com。
- 邮件交换器(MX)记录。当用户将邮件送到本地邮件服务器后，本地邮件服务器必须将邮件送到目的地邮件服务器，而目的地的邮件服务器 IP 地址可以向 DNS 服务器查询。邮件交换器记录就是指定哪些主机负责接收该区域的电子邮件，如果在此区域内创建了多个邮件交换器记录，可以调整此区域邮件服务器的优先级，数字较低的优先级较高。
- 指针(PTR)资源记录。用来记录在反向查找区域内的 IP 地址及主机。用户可通过该类型的资源记录把 IP 地址映射为主机域名。
- 起始授权机构(SOA)记录。用来记录此区域中的主要名称服务器以及管理此 DNS 服务器的管理员的电子邮件信箱。

- 名称服务器(NS)记录。用来记录管辖此区域的名称服务器，包括主域名服务器和辅助域名服务器。

2)　高速缓存初始化文件

在 Linux 系统上，通常在/var/named 目录下已经提供了一个 named.ca。该文件中包含了 Internet 的顶层域名服务器，但这个文件通常会有变化，所以建议最好从 Inter NIC(Internet 网络信息中心)下载最新的版本。该文件可以通过匿名 FTP 下载。

3)　环回地址转换文件

该文件用来说明“环回地址”的 IP 地址到主机名的映射。其文件名由/etc/named.conf 中反向环回地址区定义，通常为/var/named/named.local。该文件的内容如下：

```
$TTL  86400
@        IN   SOA     localhost.  root. localhost. (
                          2001110600  ;serial
                          28800       ;refresh
                          14400       ;retry
                          3600000     ;expire
                          86400 )     ;minimum
         IN   NS      localhost.
1        IN   PTR     localhost.
```

【说明】

- 此文件的内容是特定的，在不同域的域名服务器上，所要修改的只是 SOA 记录和 NS 记录。
- PTR 记录的最后域名为完全标识域名，以“.”结束。

4)　正向域名转换数据文件

该文件指定了域中主机域名同 IP 地址的映射，实现域名的正向解析。其文件名由/etc/named.conf 中正向域名解析区声明定义，本例中该文件名为/var/named/named.hosts。其内容如下：

```
$TTL  86400
@        IN   SOA     a100.abc.com.cn.    root.abc.com.cn. (
                      2001110600 ; serial
                      28800 ; refresh
              14400 ; retry
              3600000 ; expire
              86400 ; minimum
              )
              IN   NS   a100.abc.com.cn.
              IN   MX   10  a100.abc.com.cn.
localhost.    IN   A    127.0.0.1
a100          IN   A    210.45.12.100
a101          IN   A    210.45.12.101
www           IN   CNAME    a101
```

【说明】

- 在文件中所有的记录行都要顶格写，前面不能有空格。
- 行 IN NS a100.abc.com.cn.说明该域的域名服务器，至少应该定义一个。

- 行 IN MX 10 a100.abc.com.cn.是一条邮件交换器(MX)记录，指明了单位的邮件交换器是 a100.abc.com.cn，它负责处理邮件地址的主机部分为@abc.com.cn 的邮件，10 表示优先级别。
- 类似于行 a100 IN A 210.45.12.100 的是一系列的 A 记录，表示主机名和 IP 地址的对应关系。a100 是主机名，210.45.12.100 是它的 IP 地址。
- 行 www IN CNAME a101 表示一条定义别名的记录，即 www.abc.com.cn 和 a101.abc.com.cn 表示同一台主机。

5) 反向域名转换数据文件

该文件主要定义了 IP 地址到主机名的转换，实现域名的反向解析。IP 地址到主机名的转换是非常重要的，Internet 上的很多应用，如 NFS、Web 服务等都要用到该功能。其文件名由/etc/named.conf 中反向域名解析区声明定义，本例中其名称为/var/named/named.rev。该文件的内容如下：

```
$TTL  86400
@        IN   SOA     a100. abc.com.cn.   root. abc.com.cn. (
              2001110600 ; serial
              28800 ; refresh
              14400 ; retry
              3600000 ; expire
              86400 ; minimum
              )
         IN   NS      abc.com.cn.
100     IN    PTR     a100.abc.com.cn.
101     IN    PTR     a101.abc.com.cn.
```

【说明】

- PTR 记录用于定义 IP 地址名到主机域名的映射，即 IP 地址 210.45.12.100 对应的主机名为 a100.abc.com.cn，IP 地址 210.45.12.101 对应的主机名为 a101.abc.com.cn。
- PTR 记录的最后一项必须是一个完整的标识域名，以“.”结束。

**注意：** 在辅助域名服务器和缓存域名服务器中，不需要配置正向域名转换数据文件/var/named/named.hosts 和反向域名转换数据文件/var/named/named.rev。但在辅助域名服务器中，若不存在这两个文件，域名服务器的守护程序将自动从主域名服务器中下载这两个文件，文件内容与主域名服务器完全相同；若文件存在，则检查主域名服务器中的数据是否不同于本地文件，若有变化就下载并更新本地文件的内容；若无变化就加载本地磁盘文件，而不必从远程下载。

3. 启动、停止和重新启动域名服务器

默认安装时，域名服务器的守护程序为/etc/rc.d/init.d/named，是域名服务的最主要文件。用户可以通过该程序启动、重新启动、停止域名服务。其命令分别如下：

```
#/etc/rc.d/init.d/named start
#/etc/rc.d/init.d/named restart
#/etc/rc.d/init.d/named stop
```

如果设定 DNS 服务在计算机启动时自动启动或不启动，可以通过 chkconfig 命令来设

定。该命令格式如下：

```
chkconfig [--level <运行级>] <名字> [on|off]
```

例如，希望计算机在运行级别 3、5 的情形下启动时自动启动 DNS 服务，则命令如下：

```
#chkconfig --level 35 named on
```

再如，希望计算机在运行级别 2 的情形下启动时不启动 DNS 服务，则命令如下：

```
#chkconfig --level 2 named off
```

## 2.2.2　典型例题分析

**例 1**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题二)

**【说明】**

某单位网络拓扑结构如图 2-15 所示，FTP 服务器的域名为 xhfip.SoftwareExam.com。

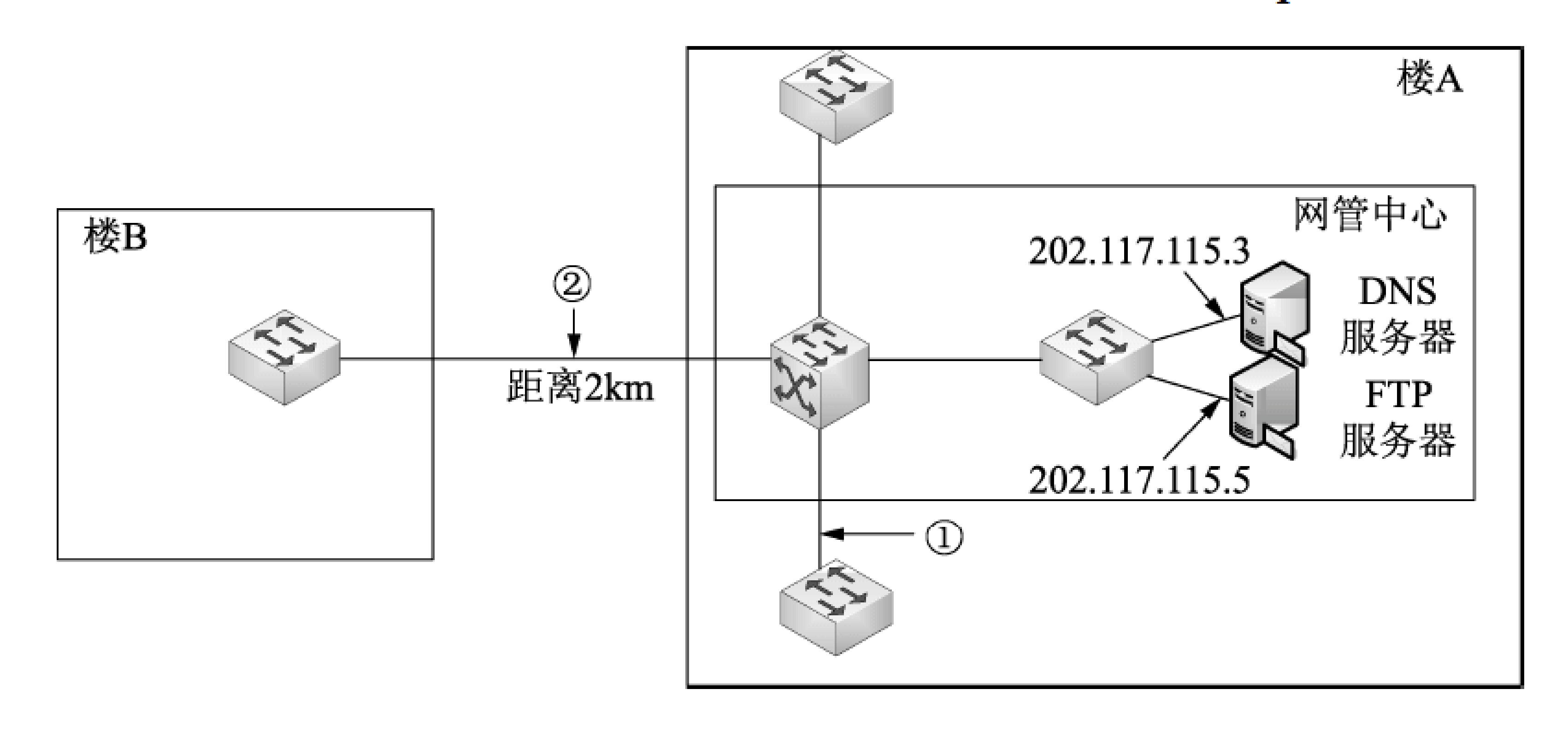


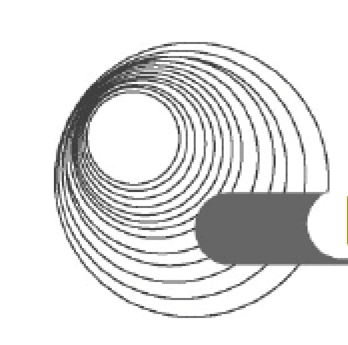

图 2-15　某单位网络拓扑结构

**【问题 1】**

依据图 2-16 配置好 FTP 服务器后，其数据端口为__(1)__，若尚未配置域名记录，在浏览器中可输入 URL__(2)__来访问 FTP 站点。




图 2-16　FTP 配置界面





【问题 2】

图 2-17 所示为用户组的权限设置，网站的创建者对 FTP 根目录的默认权限为__(3)__。




图 2-17　FTP 配置权限

【问题 3】

在 DNS 服务器中为 FTP 服务器配置域名记录时，新建主机如图 2-18 所示。

在图 2-18 所示的对话框中，添加的主机“名称”为__(4)__，“IP 地址”是__(5)__。

如果要实现 FTP 服务器的 IP 地址和域名互查，该如何操作?__(6)__




图 2-18　FTP 配置新建主机图

分析：

【问题 1】

默认情况下，FTP 服务器数据端口和控制端口分别是 20 和 21，控制端口也可手工设置

(通常为大于 1024 的高端)，若设置好控制端口，数据端口通常为控制端口−1，图 2-21 中为 FTP 服务器设置 TCP 端口为 21，故其数据端口为 20。

在没有配置域名记录的情况下，要访问该 FTP 服务器，在浏览器中可输入 URL ftp://202.117.115.5:2121 来访问 FTP 站点。

**【问题 2】**

网站的创建者需要完全控制网站，故其对 FTP 根目录的默认权限为完全控制。

**【问题 3】**

在 DNS 服务器中为 FTP 服务器配置域名记录时，由于 FTP 服务器的域名为 xhftp.SoftwareExam.com，故添加的主机“名称”为 xhftp，“IP 地址”是 202.117.115.5。

如果要实现 FTP 服务器的 IP 地址和域名互查，即 FTP 服务器除了正向解析外还需反向解析的功能，在图 1-37 中，选中“创建相关的指针(PTR)记录©”复选框实现反向解析。

答案：

**【问题 1】**

(1) 21

(2) ftp://202.117.115.5:2121

**【问题 2】**

(3) 完全控制

**【问题 3】**

(4) xhfip　(5) 222.35.40.0

(6) 选中“创建相关的指针(PTR)记录”复选框

## 2.2.3　同步练习

1．阅读以下说明，回答问题 1 至问题 5，将解答填入对应的答案栏内。

**【说明】**

某公司在国际网络互联中心申请了一个 C 类的 IP 地址 210.45.12.0/24，域名为 abc.com.cn。该公司有一台 Web 服务器(IP 地址为 210.45.12.11，主机名为 S1)、一台 FTP 服务器(IP 地址为 210.45.12.12，主机名为 S2)、一台 MAIL 服务器(IP 地址为 210.45.12.13，主机名为 S3)和一台 DNS 服务器(IP 地址为 210.45.12.14，主机名为 S4)。若你是该公司的网络管理员，使用一台装有 Windows Server 2003 的服务器作为 DNS 服务器。

**【问题 1】**该服务器必须是什么类型的 DNS 服务器？

**【问题 2】**该 DNS 服务器的正向查找区域是什么？反向查找区域是什么？

**【问题 3】**现已在正向查找区域中添加了一些主机记录，当用户的浏览器地址栏中输入 http://s1.abc.com.cn 时可以访问该公司的主页，但输入 http://www.abc.com.cn 时却不能访问该公司的主页，问题出在哪儿？如何解决？

**【问题 4】**原来该公司用户的电子邮件地址格式是 xxx@mail.abc.com.cn，现在想把它改为 xxx@abc.com.cn，除了在邮件服务器上做修改之外，在域名服务器上还要做哪些修改？

**【问题 5】**现在反向查找区域添加了一个指针(PTR)记录，该记录的作用是什么？

2．回答问题 1 至问题 3，将解答填入对应的答案栏内。

【问题 1】DNS 的作用是什么？

【问题 2】Internet 中的域名是如何组织的？

【问题 3】Internet 域名解析有哪两种方式？

### 2.2.4 同步练习参考答案

1．

【问题 1】主域名服务器。

【问题 2】abc.com.cn、12.45.210.in-addr.arpa。

【问题 3】可能是没有将 s1.abc.com.cn 的别名设置为 www.abc.com.cn，或者设置不正确。可以在正向查找区域中增加一条别名(CNAME)记录，使真实主机名为 s1.abc.com.cn，别名为 www.abc.com.cn。

【问题 4】在正向查找区域中删除原有的邮件交换器记录(MX)，新建一条邮件交换器记录(MX)，在“主机或域名”处不要填写任何内容，服务器地址设置为 s3.abc.com.cn。

【问题 5】实现 IP 地址向域名的映射。

2．

【问题 1】DNS 的作用是将符号化的域名映射为 IP 地址。

【问题 2】Internet 中的域名是按树形结构组织的。

【问题 3】Internet 域名解析有递归解析和迭代解析两种方式。

## 2.3 FTP 服务器

### 2.3.1 考点辅导

#### 2.3.1.1 Windows Server 2008 R2 的 IIS 下 FTP 服务器的安装与设置

Windows Server 2008 R2 中的 IIS 里内置 FTP 服务模块，安装比较简单。在 FTP 服务安装过程中，安装程序会自动创建一个“默认 FTP 站点”，可以直接修改该站点的属性来满足应用需求。为了更好地管理 FTP 服务器，需要对它进行适当的配置。

在 Internet 信息服务控制台下，右击“默认 FTP”选项，在弹出的快捷菜单中选择“属性”命令，弹出“默认 FTP 站点属性”对话框，如图 2-19 所示。对于“FTP 站点”“安全帐户”“主目录”和“目录安全性”的设置基本上与 Web 站点相似，这里就不再赘述了。下面着重介绍“消息”选项卡中的相关设置，打开“消息”选项卡，如图 2-20 所示。





图 2-19　FTP 站点属性




图 2-20　“消息”选项卡

FTP 站点消息的相关设置如表 2-3 所示。

表 2-3　FTP 消息设置

| 配 置 项 | 说　明 |
| --- | --- |
| 标题 | FTP 的站点名称，用户在登录 FTP 时显示的信息 |
| 欢迎 | 用户登录 FTP 时显示的信息 |
| 退出 | 当用户退出 FTP 时显示的信息 |
| 最大连接数 | 当 FTP 服务器超过最大连接人数时，给提出连接请求的客户机发送一条错误信息 |

由于服务器配置、性能等的差别，有些服务器不能满足大访问量的需要，往往造成超时甚至死机，因此需要设置连接限制。在图 2-19 所示的“FTP 站点连接”选项组中，有 3 个选项可供选择。

不受限制：该选项允许同时发生的连接数将不受任何限制。

连接限制为：该选项限制允许同时发生的连接数为某一特定值，这一特定值由用户在文本框中输入。

连接超时：当某条 FTP 连接在一段时间内没有反应时，服务器就自动断开该连接。

#### 2.3.1.2　Linux 下 Wu-FTP 服务器的安装与配置

在 Linux 环境下使用的 FTP 服务器软件主要有 Wu-FTP、NcFTP 和 ProFTP 等 3 种。由于 Wu-FTP 是目前最流行的一种免费 FTP 服务器软件，所以下面主要介绍 Wu-FTP。

1. Wu-FTP 功能和特征

1)　Wu-FTP 的特征

(1)　Wu-FTP 是基于 GPL 协议开发的，它是一个源代码公开的自由软件。

(2)　Wu-FTP 是历史最久的非商业 FTP 服务器程序之一，它的影响非常广泛。

(3)　Wu-FTP 项目仍然继续进行，新的特性不断被加入。

(4)　Wu-FTP 支持广泛的 UNIX 和类 UNIX 平台。

2)　Wu-FTP 的功能

(1)　可以控制不同网络和域的用户对 FTP 服务器的存取权限和访问时段。

(2) 使用者在下载文件时，可以自动对其进行压缩和解压缩工作。
(3) 可以记录文件上传和下载的全过程。
(4) 可以显示传输时的相关信息，方便用户及时了解目前的传输动态。
(5) 可以设置最大连接数，从而提高了效率，且有效地控制了负载。
(6) 可以暂时关闭 FTP 服务器，以便系统维护。

2. Wu-FTP 服务器的获取与安装

Wu-FTP 有 RPM 包分发版本，可以从 Red Hat 网站下载或在 Red Hat Linux 7.0 的光盘中找到。二进制的分发版本可以从 ftp://ftp.wu-ftpd.org/pub/wuftpd 处进行下载。

下面以 RPM 的安装为例介绍 Wu-FTP 的安装过程。

若在安装 Red Hat 时没有安装 Wu-FTP，则可以使用下面的命令进行安装：

```
#rpm -ivh wu-ftpd-2.6.0.i386.rpm
```

若获得了更新版本的 Wu-FTP 的 RPM，可以使用下面的命令进行升级：

```
#rpm -Uvh wu-ftpd-2.6.x.i386.rpm
```

当安装完成后，系统中将存在表 2-4 所示的文件。

表 2-4 Wu-FTP 的主要文件

| 类 型 | 文 件 名 | 说 明 |
|---|---|---|
| 可执行文件 | /usr/bin/ftpcount | 显示目前在线人数 |
| | /usr/bin/ftpwho | 查看目前 FTP 服务器的连接情况 |
| | /usr/sbin/ckconfig | 检查设置是否正确 |
| | /usr/sbin/ftprestart | 重新启动 FTP 服务器 |
| | /usr/sbin/ftpshut | 用于关闭服务程序 |
| | /usr/sbin/in.wuftpd | FTP 服务程序 |
| | /usr/sbin/privatepw | 改变 Wu-FTP 组访问文件 |
| 配置文件 | /etc/ftpaccess | Wu-FTP 的主配置文件，控制存取权限 |
| | /etc/ftpconversions | 用来控制当传输文件时是否进行压缩 |
| | /etc/ftpusers | 禁止某些用户登录 |
| | /etc/ftphosts | 禁止某些来自指定机器上的登录 |
| | /etc/ftpgroups | 创建用户组，这个组中的成员预先定义可以访问 FTP 服务器 |
| 手册 | /usr/share/doc/wu-ftpd-2.6.1/ | 存放 Wu-FTP 手册页 |
| 文档 | /usr/share/man/ | 存放 Wu-FTP 文档 |

3. 启动 Wu-FTP

1) 修改/etc/services

需要确定/etc/services 文件有以下一行内容，同时该内容未被加上注释符“#”：

```
ftp          21/ftp      ftp
```

2)　创建/etc/xinetd.d/wu-ftpd 文件

文件大致内容如下：

```
service ftp
{
disable                 = no
socket_type             = stream
wait                    = no
user                    = root
server                  = /usr/sbin/in.ftpd
server_args             = -l -a
log_on_success          += DURATION USERID
log_on_failure          += USERID
nice                    =10
}
```

3)　重新启动 xinetd

要想使修改内容立即生效，可以重新启动 xinetd 程序。其命令如下：

```
#/etc/rc.d/init.d/xinetd restart
```

4)　测试 Wu-FTP 是否启动

与测试 Sendmail 服务器一样，可以通过 telnet 命令登录到 21 端口来测试 Wu-FTP 服务是否启动。其命令如下：

```
#telnet localhost 21
```

如果登录成功，则表明该服务器已成功安装并启动。

4.　Wu-FTP 服务器的配置

1)　/etc/ftpuser 的配置

/etc/ftpuser 用来指定某些用户不能登录本 FTP 服务器。其实这个设置是十分简单的，只需将要禁止的用户账号写入文件/etc/ftpuser 中。由于从系统的安全考虑，一般不希望权限过大的用户和一些与命令名相同的用户进入 FTP 服务器，所以在默认配置中以下用户已经被列入了“黑名单”：

```
root
uucp
news
bin
adm
nobody
lp
sync
shutdown
halt
mail
```

2) /etc/ftphosts 的配置

/etc/ftphosts 用来指定某些主机不能连接本 FTP 服务器。要禁止某些来自指定机器上的登录有两种方法：一种是在/etc/ftpaccess 中设置 deny 命令；另一种是在/etc/ftphosts 中写入要禁止的主机的 IP 地址或域名。下面是一个/etc/ftphosts 文件的范例：

```
allow xyz *.abc.com.cn 210.102.0.0/16
deny tom *.hanker.com 131.222.154.0/24
```

例中允许用户 xyz 从域名以 abc.com.cn 为后缀的主机及 210.102.0.0/255.255.0.0 的主机上登录；禁止用户 Tom 从域名 hanker.com 为后缀的主机及 131.222.154.0/255.255.255.0 的主机上登录。当用户名为 anonymous 或 ftp 时，均表示匿名用户。

3) /etc/ftpconversions 的配置

/etc/ftpconversions 文件主要定义用户从 FTP 服务器中下载文件时对文件进行格式转换的规则，如压缩、解压缩、打包和开包等操作。这样用户就不必为.tar、.gz、.tgz、.Z、.z 之类的文件伤脑筋了。

/etc/ftpconversions 文件的格式乍看上去很复杂，不过不必担心，基本上不用修改、设置。下面是一个/etc/ftpconversions 文件，它已经能够满足一般的使用需要了。

```
:.Z: : :/bin/compress -d -c %s:T_REG|T_ASCII:O_UNCOMPRESS:UNCOMPRESS
: : :.Z:/bin/compress -c %s:T_REG:O_COMPRESS:COMPRESS
:.gz: : :/bin/gzip -cd %s:T_REG|T_ASCII:O_UNCOMPRESS:GUNZIP
: : :.gz:/bin/gzip -9 -c %s:T_REG:O_COMPRESS:GZIP
: : :.tar:/bin/tar -c -f - %s:T_REG|T_DIR:O_TAR:TAR
: : :.tar.Z:/bin/tar -c -Z -f - s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+COMPRESS
: : :.tar.gz:/bin/tar -c -z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR+GZIP
```

如果想让 FTP 服务器有自动压缩、解压缩的功能，必须先将一些压缩、解压缩的命令文件如 tar、gzip、gunzip、compress、uncompress 等复制到/home/ftpd/bin 目录下。

4) /etc/ftpaccess 的配置

/etc/ftpaccess 是 FTP 服务器上最重要的配置文件，它主要控制 FTP 存取权限，直接关系到 FTP 服务器能否正常工作，还有其他许多权限上的设置。下面是一个典型的配置实例。

```
loginfails 3
class local real *
class remote anonymous guest *
limit remote 100 Any /etc/ftpd/toomany.msg
message /etc/ftpd/welcome.msg login
compress yes local remote
tar yes local remote
private yes
passwd-check rfc822 warn
log commands real
log transfer anonymous guest inbound outbound
log transfer real inbound
shutdown /etc/ftpd/shut.msg
delete no anonymous,guest
overwrite no anonymous,guest
```

```
rename no anonymous
chmod no anonymous,guest
umask no anonymous
upload /home/ftpd * no
upload /home/ftpd /bin no
upload /home/ftpd /etc no
upload /home/ftpd /pub yes real 0644 dirs
upload /home/ftpd /incoming yes real guest anonymous 0644 dirs
alias inc /incoming
email guest@xxx.net
email guest@yyy.net
deny *.com.tw /etc/ftpd/deny.msg
```

下面逐条进行讲解，并给出每条设置的含义，以便读者触类旁通，根据自己 FTP 服务器的具体情况进行合理设置。

(1)　登录重试次数。

格式：loginfails [次数]

功能：设置当用户登录到 FTP 服务器时，允许用户输入错误密码的次数。

实例：loginfails 3，密码输入错误 3 次就切断连接。

(2)　定义用户类别。

格式：class [类名] [real/guest/anonymous] [IP 地址]

功能：用于设置 FTP 服务器上用户的类别，并可对客户端的 IP 地址进行限制，允许某部分的 IP 地址或全部的 IP 地址访问。而在 FTP 服务器上的用户基本上可以分为以下 3 类。

①　real：在该 FTP 服务器有合法账号的用户。

②　guest：有记录的匿名用户。

③　anonymous：权限最低的匿名用户。实例如下。

class local real *：定义一个名为 local 的类，它包括在任何地方登录(*代表所有 IP 地址)的 real 用户。

class remote anonymous guest *：定义一个名为 remote 的类，它包括在任何地方登录的 anonymous 用户和 guest 用户。

(3)　登录人数的限制。

格式：limit [类别] [人数] [时间] [文件名]

功能：设置指定时间内指定的类别允许连接的人数上限，当达到人数上限时显示指定文件的内容。

实例：limit remote 100 Any/etc/ftpd/toomany.msg　在任何时间内，remote 类的访问用户达到 100 人时，将不再允许或无法产生新的连接。当第 101 位用户要连接时，连接将失败，并向用户显示文件/etc/ftpd/toomany.msg 的内容。

(4)　用户登录时显示的文件。

格式：message [文件名称] [指令]

功能：当用户执行指定的指令时，系统将指定的文件内容显示出来。

实例：message/etc/ftpd/welcome.msg login　当用户执行 login 命令时，也就是登录到 FTP 服务器上的时候，系统将显示文件/etc/ftpd/welcome.msg 的内容。

(5) 压缩功能。

格式：compress [yes/no] [类别]

功能：设置某个类别的用户可以使用 compress(压缩)功能。

实例：compress yes local remote　允许 local 和 remote 两类用户都能使用 compress(压缩)功能。

(6) 归档功能。

格式：tar [yes/no] [类别]

功能：设置某个类别的用户可以使用 tar(归档)功能。

实例：tar yes local remote　允许 local 和 remote 两类用户都能使用 tar 功能。

(7) 是否支持群组。

格式：private [yes/no]

功能：设置是否支持群组对文件的取用。

实例：private yes　支持群组对文件的取用。

(8) 匿名用户密码检查。

格式：passwd-check [none/trivial/rfc822] [enforce/warn]

功能：设置匿名用户 anonymous 的密码使用方式。

none 表示不做密码验证，任何密码都可以登录。

trivial 表示只要输入的密码中含有字符“@”就可以登录。

rfc822 表示密码一定要符合 RFC 822 中所规定的 E-mail 地址才能登录。

enforce 表示输入的密码不符合以上指定的格式就不允许登录。

warn 表示密码不符合规定时只出现警告信息，仍然能够登录。

实例：passwd-check rfc822 warn　希望能够得到符合规定的 E-mail 作为密码，但如果不是也允许登录。

(9) 操作日志。

格式：log command [real/guest/anonymous]

功能：设置某些用户登录后的操作记录在文件/usr/adm/xferlog 中。

实例：log command real　当 real 用户登录后，将其操作记录下来。由于其他用户权限较低，所以操作不会引起太大的安全隐患，所以一般只需记下 real 用户的操作就可以了。

(10) 文件传送日志。

格式：log transfer [real/guest/anonymous] [inbound/outbound]

功能：设置某些用户的上传(Inbound)和下载(Outbound)操作日志。

实例：

log transfer anonymous guest inbound outbound　对于匿名用户要更加关注他们的文件操作，所以无论是上传还是下载都进行记录。

log transfer real inbound：对于合法用户则只记录他的上传记录。

(11) FTP 服务器关闭设置文件。

格式：shutdown [文件名]

功能：FTP 服务器关闭的时间可以设置在后面所指定的文件中，当设置的时间一到，便无法登录 FTP 服务器了，要想恢复，只有将这个文件删掉。而这个文件必须由指令

/bin/ftpshut 来生成。

实例：shutdown /etc/ftpd/shut.msg

(12) 删除文件权限设置。

格式：delete [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 delete 命令删除文件。默认是允许。

实例：delete no anonymous,guest　为了更好地管理 FTP 服务器，一般情况下不允许匿名用户执行 delete 命令。

(13) 覆盖文件权限设置。

格式：overwrite [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户覆盖同名文件。默认是允许。

实例：overwrite no anonymous,guest　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户覆盖同名文件。

(14) 文件改名权限设置。

格式：rename [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 rename 命令来为文件改名。默认是允许。

实例：rename no anonymous　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 rename 命令改变文件名。而对有记录的匿名用户则适当放宽，允许他们使用改名命令。

(15) chmod 命令权限设置。

格式：chmod [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 chmod 命令更改文件权限。默认是允许。

实例：chmod no anonymous, guest　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 chmod 命令更改文件权限。

(16) umask 命令权限。

格式：umask [yes/no] [real/anonymous/guest]

功能：设置是否允许指定用户使用 umask 命令。默认是允许。

实例：umask no anonymous　为了更好地管理 FTP 服务器，一般情况下，不允许匿名用户执行 umask 命令。

(17) 用户上载目录。

格式：upload [根目录] [上传目录] [yes/no] [用户] [权限] [dirs/nodirs]

功能：对可以上传的目录进行更加详细的设置。

实例：

upload /home/ftpd * no　表示在子目录/home/ftpd 下不允许上传。

upload /home/ftpd /bin no　表示在子目录/home/ftpd/bin 下不允许上传。

upload /home/ftpd /etc no　表示在子目录/home/ftpd/etc 下不允许上传。

upload/home/ftpd/pub yes real 0644 dirs　允许服务器上的合法用户在子目录/home /ftpd/pub 下可以上传权限为 0644(也就是-rw-r--r--)的文件，而且在这个目录下可以新建子目录。

upload /home/ftpd /incoming yes real guest anonymous 0644 dirs　允许所有的用户在子目

录/home/ftpd/incoming 下可以上传权限为 0644 的文件，而且在这个目录下可以新建子目录。

(18) 虚拟目录。

格式：alias [目录别名] [目录名]

功能：为指定目录设置一个别名，在切换目录时就可以使用较短的目录别名。

实例：alias inc：/incoming　为子目录 incoming 设置一个别名 inc。

(19) 管理员的 E-mail 地址。

格式：email [guest 的 E-mail 地址]

功能：只要在此设置系统管理员的 E-mail 地址，FTP 服务器有问题或任何信息都要通知系统管理员。

实例：email guest@XXX.net　这里仅是一个示例，实际上可以包含多个符合规范的 E-mail 地址。

(20) 访问限制。

格式：deny [IP 地址/域名] [说明文件]

功能：可以限制某些 IP 地址或域名的用户无法登录 FTP 服务器。

实例：deny *.com.tw/etc/ftpd/deny.msg　设置凡是以.com.tw 结束的域名，都禁止其访问。而将/etc/ftpd/deny.msg 的内容显示给用户看。

5. 与 Wu-FTP 相关的其他一些命令的使用

1) 连接数字统计命令 ftpcount

使用 ftpcount 命令可以十分清楚地统计出当前连接到 FTP 服务器上的用户数，并且同时列出上限。命令输出如下：

```
#ftpcount
Service class local    -  0   users   (20     maximum)
Service class remote   -  5   users   (100    maximum)
```

上例中显示属于 local(本地)的有 0 个人在线，上限为 20；属于 remote(远程)的有 5 个人在线，上限为 100。

2) 在线用户查看命令 ftpwho

使用 ftpwho 命令可以查看当前连接用户的详细情况。命令输入如下：

```
#ftpwho
Service class all:
ftp     12586   536 0   21:58 ? 00:00:00 ftpd: abc.com.cn :anonymous
ma      12557   532 0   21:58 ? 00:00:00 ftpd: localhost:ma:IDLE
-2  users (no maximum)
```

上例中显示 all 类有两个用户登录，并显示登录时间、来源和状态。

3) FTP 关闭文件生成命令 ftpshut

可以使用 ftpshut 命令生成一个在目录/etc/ftpaccess 中设置的 shut.msg 文件，用于关机设定。ftpshut 命令的格式如下：

```
#ftpshut [-l<分钟>][-d<分钟>] [关闭时间] ["警告信息"]
```

- -l<分钟>：指定在关闭 FTP 服务器功能前多少分钟时停止用户的连接。

- -d<分钟>：指定在关闭 FTP 服务器功能前多少分钟时切断用户连接。
- 关闭时间：指定关闭 FTP 服务器的时间，如 6:20 写为 0620。如果要立即关闭，可以用 now。
- "警告信息"：指定断线之前显示给用户的警告信息。

下面是 ftpshut 运行实例：

```
#ftpshut -l25 -d5 2300 "Warn: FTP server will shutdown!"
#cat /etc/shutmsg
2001    18  23  00  0025    0005
Warn:FTP server will shutdown!
```

例子中的 FTP 服务器将在 23:00 关闭，关闭前 25 分钟将拒绝用户登录，关闭前 5 分钟将断开所有连接，并给在线用户发送“Warn:FTP server will shutdown!”消息。

如果要立即关闭 FTP 服务器，则输入：

```
#ftpshut now
```

FTP 服务器关闭后要重新启动，只要把目录/etc/shutmsg 下的这个文件删除，并重新启动 FTP 服务器就可以继续 FTP 服务了。

## 2.3.2　典型例题分析

**例 1**　阅读以下说明，回答问题 1 至问题 5，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题二)

**【说明】**

某单位网络拓扑结构如图 2-21 所示，FTP 服务器的域名为 xhfip.SoftwareExam.com。

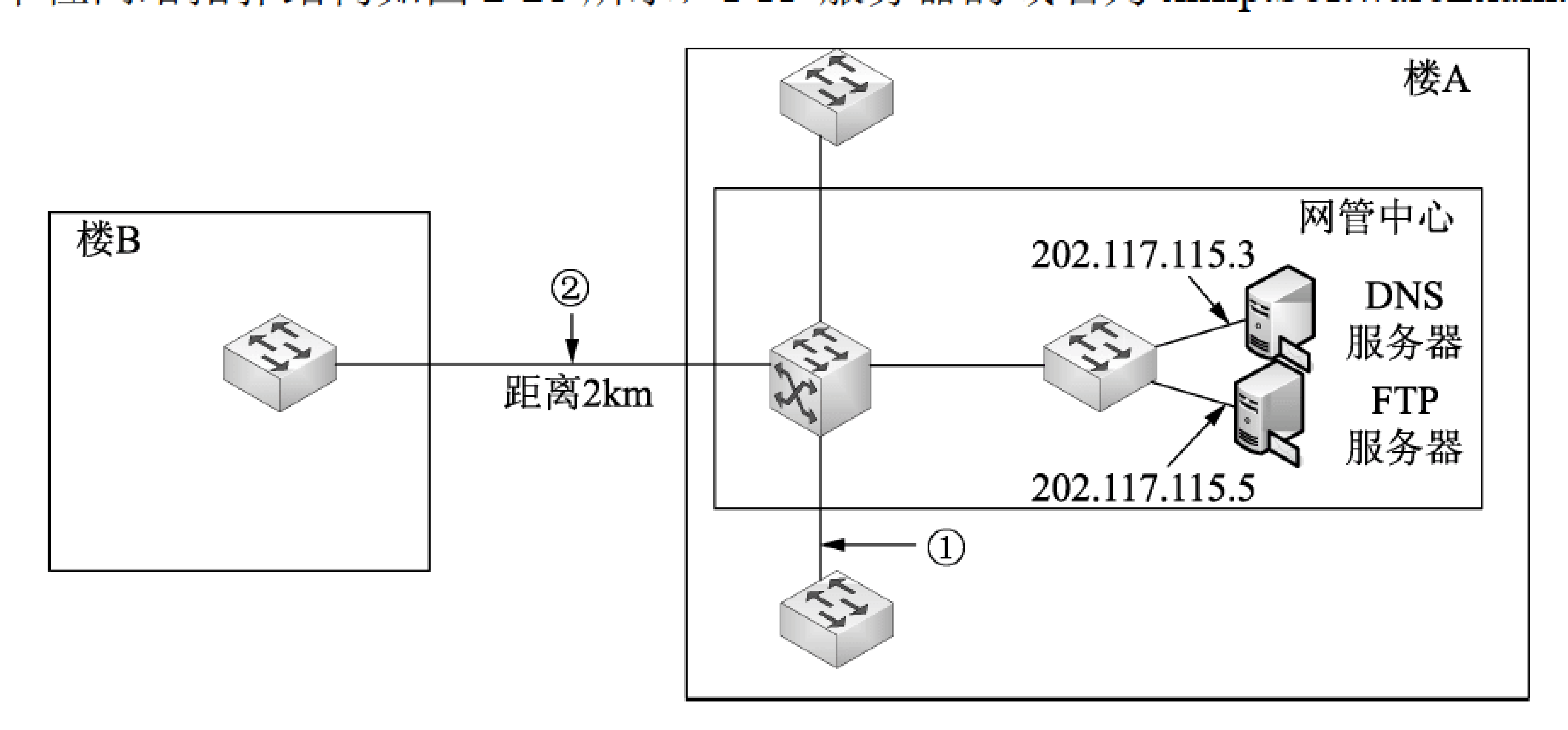



**图 2-21　某单位网络拓扑结构**

**【问题 1】**(2 分)

在该单位综合布线时，连接楼 A 与楼 B 的布线子系统为__(1)__；楼 A 内网管中心服务器群至核心交换机的布线子系统为__(2)__。

(1)、(2)备选答案：

A. 水平子系统　　B. 垂直子系统　　C. 设备间子系统

D. 建筑群子系统　　E. 干线子系统　　F. 管理子系统

【问题 2】(4 分)

图 2-21 中①的传输介质为__(3)__，②的传输介质为__(4)__。

(3)、(4)备选答案(限选一次)：

A. 单模光纤　　B. 多模光纤

【问题 3】(2 分)

依据图 2-22 配置好 FTP 服务器后，其数据端口为__(5)__，若尚未配置域名记录，在浏览器中可输入 URL__(6)__来访问 FTP 站点。




图 2-22　FTP 服务器配置

【问题 4】(4 分)

图 2-23 所示为用户组的权限设置，网站的创建者对 FTP 根目录的默认权限为__(7)__。




图 2-23　FTP 服务器配置权限设置

**【问题 5】**(3 分)

在 DNS 服务器中为 FTP 服务器配置域名记录时，新建主机如图 2-24 所示。

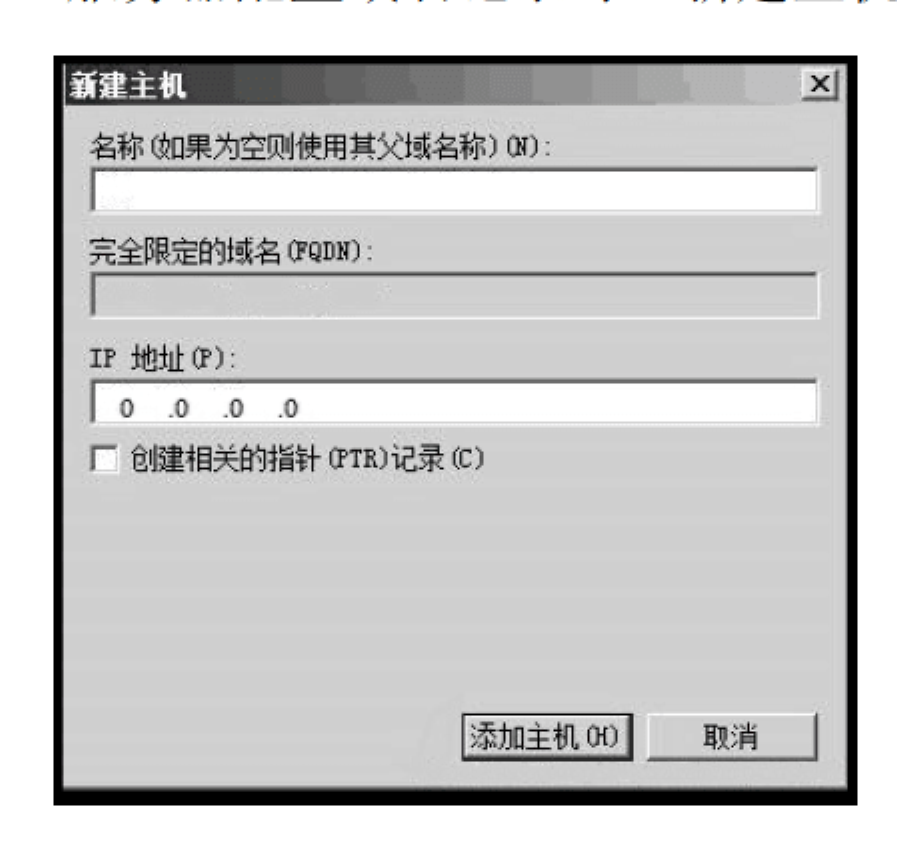



图 2-24　FTP 服务器配置新建主机图

在图 2-24 所示的对话框中，添加的主机“名称”为__(8)__，“IP 地址”是__(9)__。如果要实现 FTP 服务器的 IP 地址和域名互查，该如何操作？__(10)__

**分析：**

本试题考查综合布线、用户权限以及服务器配置相关知识，属传统考查项目。

**【问题 1】**

综合布线系统由 6 个子系统组成，即建筑群子系统、设备间子系统、干线子系统、管理子系统、配线子系统、工作区子系统。大型布线系统需要用铜介质和光纤介质部件将 6 个子系统集成在一起 。

(1) 水平子系统(Horizontal Subsystem)：由信息插座、配线电缆或光纤、配线设备和跳线等组成。国内称之为配线子系统。

(2) 垂直子系统(Backbone Subsystem)：由配线设备、干线电缆或光纤、跳线等组成。国内称之为干线子系统。

(3) 工作区子系统(Workarea Subsystem)：为需要设置终端设备的独立区域。

(4) 管理子系统(Administration Subsystem)：针对设备间、交接间、工作区的配线设备、缆线、信息插座等设施进行管理的系统。

(5) 设备间子系统(Equipment Room Subsystem)：安装各种设备的场所，对综合布线而言，还包括安装的配线设备。

(6) 建筑群子系统(Campus Subsystem)：由配线设备、建筑物之间的干线电缆或光纤、跳线等组成。

由此，题目中连接楼 A 与楼 B 的布线子系统为建筑群子系统；楼 A 内网管中心服务器群至核心交换机的布线子系统为设备间子系统。

**【问题 2】**

图 2-21 中①处传输介质连接两个楼层，可选多模光纤，②处连接两个建筑物，且距离 2km，故传输介质为单模光纤。

**【问题 3】**

默认情况下，FTP 服务器数据端口和控制端口分别是 20 和 21，控制端口也可手工设置

(通常为大于1024的高端)，若设置好控制端口，数据端口通常为控制端口−1，图2-22中为FTP服务器设置TCP端口为21，故其数据端口为20。

在没有配置域名记录的情况下，要访问该FTP服务器，在浏览器中可输入URL ftp://202.117.115.5:2121来访问FTP站点。

【问题4】

网站的创建者需要完全控制网站，故其对FTP根目录的默认权限为完全控制。

【问题5】

在DNS服务器中为FTP服务器配置域名记录时，由于FTP服务器的域名为xhftp.SoftwareExam.com，故添加的主机“名称”为xhftp，“IP地址”是202.117.115.5。

如果要实现FTP服务器的IP地址和域名互查，即FTP服务器除了正向解析外还需反向解析的功能，在图2-24中，选中“创建相关的指针(PTR)记录(C)”复选框可实现反向解析。

答案：

【问题1】

(1) D

(2) C

【问题2】

(3) B

(4) A

【问题3】

(5) 20

(6) ftp://202.117.115.5:21

【问题4】

(7) 完全控制

【问题5】

(8) xhfip

(9) 202.117.115.5

(10) 选中“创建相关的指针(PTR)记录”复选框

**例2** 阅读以下说明，回答问题1至问题4，将解答填入答题纸对应的解答栏内。(2016年5月下午试题二)

【说明】

某公司采用Windows Server 2008 R2配置Web服务器和FTP站点。

【问题1】

添加服务组件如图2-25所示。

在Windows Server 2008 R2操作系统中，要安装Web和FTP服务器，首先在图2-26中选中__(1)__，然后再安装__(2)__组件。

若图2-25选中证书服务可以安装CA证书。CA证书实现__(3)__和__(4)__功能。

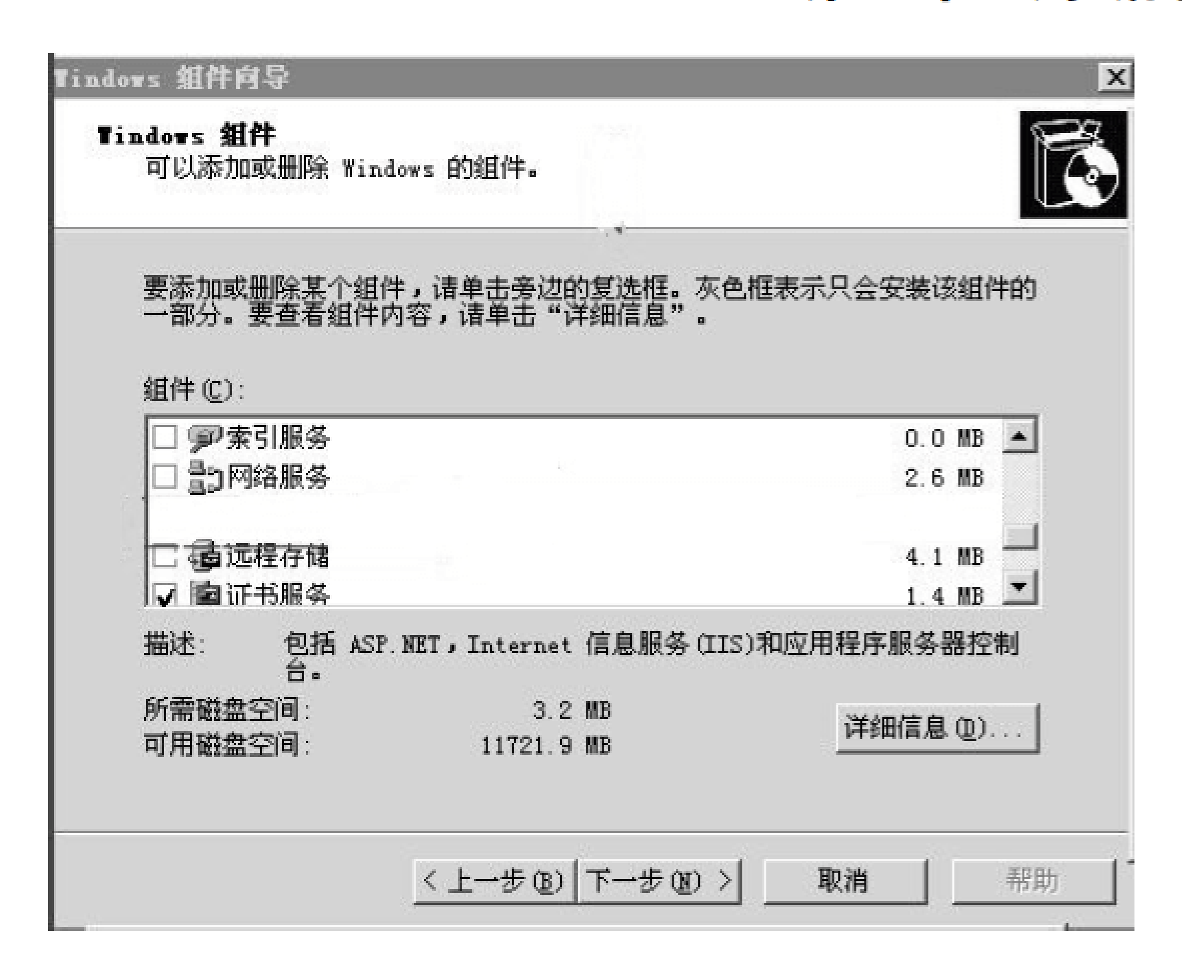



图 2-25　服务器配置图

**【问题 2】**

Web 的配置如图 2-26 所示。




图 2-26　Web 的配置

根据图 2-26 所示的配置信息判断正误(正确的答“对”，错误的答“错”)。

A．在 IP 地址下拉框中只有本机网卡对应的地址。__(5)__

B．IP 地址和服务器的网卡地址相互对应，在服务器有多块网卡时才可以配置多个地址。__(6)__

C．TCP 端口不能为空，若要更改端口号，需要通知客户端。__(7)__

D．SSL 是安全套接层协议，默认端口是 110。__(8)__

E．当该服务器 2 分钟内不能响应客户机的 Web 请求时，断开连接。__(9)__

F．客户端可以使用 127.0.0.1 访问该服务器。__(10)__

**【问题 3】**

FTP 的配置如图 2-27 所示。

1．当客户机连接到 FTP 服务器时，客户端显示的消息为__(11)__。

2．常用的 FTP 访问方式有 3 种类型：__(12)__、__(13)__、__(14)__。




图 2-27　FTP 服务器配置图

**【问题 4】**

Windows Server 2008 R2 调整工作环境的对话框如图 2-28、图 2-29 所示。

图 2-28 所示“调整以优化性能”选项中“程序”调整的是__(15)__，“后台服务”调整的是__(16)__。

(15)～(16)备选答案：

A．用户启动的应用程序，如 Word

B．用户启动的应用程序，如 DNS

C．系统运行的各种服务，如 Web

D．系统运行的各种服务，如 QQ

图 2-29 中用户变量__(17)__生效，系统变量__(18)__生效。

(17)～(18)备选答案：

A．只对 Administrator 用户

B．对所有用户

C．对各自用户

D．对除 Administrator 外的其他用户




图 2-28　“性能选项”对话框




图 2-29　“环境变量”对话框

**分析**：本题考查 Windows Server 2008 R2 网络配置的相关知识。

此类题目要求考生了解 Windows Server 2008 R2 网络服务的配置、熟悉配置界面和相关参数配置的含义。本题主要考察 WEB、FTP 配置以及系统优化的基础知识，要求考生具有网络服务配置的实际经验。

**【问题 1】**

要将万维网服务在网上发布，在 Windows 系统中是通过 IIS，在 Linux 系统中是通过 Apache 来实现的。IIS 服务在 Windows 系统中默认未安装，需要通过 Windows 组件向导程序进行添加。IIS 服务包含在“应用服务器”组件中，在该组件中还包含一系列的子组件，其中 Internet 信息服务(IIS)是其中的一类，可提供万维网服务、文件传输、邮件服务，以及新闻组等。

CA(Certificate Authority)也称为“证书授权中心”，在 Windows 系统中是通过证书服务组件实现的。证书本质上是由证书签证机关(CA)签发，对用户的公钥进行认证。为了保证信息在传输中的不被窃听，需要对证书进行加密操作。

**【问题 2】**

127.0.0.1 是回送地址，localhost 是回路网络接口(loopback)，用来测试网路层的 IP 连通性。回送地址只能用于本机测试，即程序使用回送地址发送数据，协议软件立即返回，不进行任何网络传输。在网络设置中，可以对一块网络网卡配置多个 IP 地址实现对多种网络服务的支持。当在 Web 服务中更改了 TCP 默认端口号，需要通知客户端在访问时要指明变更后的端口号，否则不能实现网站的访问。

**【问题 3】**

FTP 的任务是从一台计算机将文件传送到另一台计算机，不受操作系统的限制。FTP 默认 TCP 端口号为 21，Port 方式数据端口为 20。

FTP 提供服务时通常需要在远程文件传输的计算机上安装和运行 FTP 客户端，客户端一般使用第三方程序。使用浏览器也可以访问 FTP 服务，用户只需浏览地址栏中输入 FTP 服务器的 url 地址即可。除了上述方法外，客户端还可以通过在 Windows 系统命令窗口中输入 ftp 命令的方式实现与 FTP 服务器的连接。

**【问题 4】**

Windows 操作系统中，程序和后台服务都是指在计算机运行的程序。在对外提供网络服务时，相关服务驻留在系统“后台”，因此需要优化的是系统的“后台服务”性能。Windows 操作系统中“系统变量”对所有用户起效，“用户变量”只对当前登录系统的用户起效。

**答案**：

**【问题 1】**

(1) 应用程序服务器　　(2) IIS　　(3)加密　　(4) 认证

注：(3)、(4)可互换

**【问题 2】**

(5) 错　(6) 错　(7) 对　(8) 错　(9) 错　(10) 错

【问题 3】

(11) 欢迎光临！　　(12) 命令行

(13) 浏览器　　(14) 客户端软件

注：(12)、(13)、(14)可互换

【问题 4】

(15) A　　(16) C

(17) C　　(18) B

## 2.3.3 同步练习

1．阅读以下说明，回答问题 1～问题 4，将答案填入对应的答案栏内。

【说明】

某公司使用一台装有 Windows Server 2008 R2 的 PC 服务器作为 Web 服务器(文档的主目录为 D:\www/root)。为了使 Web 管理员(其用户名为 webadmin)能够上传主页，系统管理员在这台服务器上安装了 IIS 并配置了 FTP 服务。为了信息安全，必须对这台服务器的 FTP 作一些控制。下面是一些要求，请回答如何设置。

【问题 1】不使用 FTP 默认 TCP 端口 21 作为服务器端口，而改用 TCP 端口 8089。

【问题 2】禁止匿名用户访问该台服务器上的 FTP 服务。

【问题 3】只能在 IP 地址为 210.45.12.31 的主机上上传或下载主页数据。

【问题 4】如果想要用户 webadmin 使用 FTP 登录时，直接进入 Web 服务器的文档主目录。

2．阅读以下说明，回答问题 1～问题 4，将答案填入对应的答案栏内。

【说明】

某公司使用一台装有 Windows Server 2008 R2 的 PC 服务器作为 FTP 服务器，主要用于内部文件下载。该公司的网络地址是 192.168.10.0/24 这个 C 类地址，内部文件都存放在“D:\公用文件”下，另外每个用户都在该服务器上有一个账号和自己的主文件夹(主文件夹都不在“D:\公用文件”下)。

【问题 1】若该公司内部所有的用户使用匿名用户就可以下载内部文件，FTP 站点主目录设置成什么？如何设置？

【问题 2】为保证外网的用户不能访问该 FTP 站点，如何设置？

【问题 3】由于该服务器还提供其他服务，必须限制最大在线人数为 100，如何实现这一功能？

【问题 4】如果想让每个用户使用自己的账号登录该服务器时，就直接进入自己的主文件夹，如何实现这一功能？

## 2.3.4 同步练习参考答案

1．

【问题 1】打开 FTP 站点属性窗口，在“FTP 站点”选项卡的“TCP 端口”文本框中

将 21 改为 8089，再重新启动 FTP 服务。

**【问题 2】**在“安全账户”选项卡中，取消选中“允许匿名连接”复选框，即可禁止用户匿名访问该 FTP 站点。

**【问题 3】**在“目录安全性”选项卡中，选中“拒绝访问”单选按钮，单击“添加”按钮，在弹出的对话框中，选中“单机”单选按钮，再在“IP 地址”文本框中输入 210.45.12.31。

**【问题 4】**新建一个别名为 webadmin 的虚拟目录，其实际位置为 D:\wwwroot，并将访问权限设置为“读取”和“写入”。

2.

**【问题 1】**主目录应设置为“D:\公用文件”。操作步骤是：在 FTP 站点的属性窗口中，切换到“主目录”选项卡，选中“此计算机上的目录”单选按钮；在“FTP 站点目录”选项区域中，单击“浏览”按钮，选择“D:\公用文件”，或者直接输入“D:\公用文件”。

**【问题 2】**设置目录安全性的具体操作步骤是：在 FTP 站点的属性窗口中切换到“目录安全性”选项卡，选中“拒绝访问”单选按钮，单击“添加”按钮；在“授权以下访问”对话框中，选中“一组计算机”单选按钮，在“网络标识”文本框中输入 192.168.10.0，在“子网掩码”文本框中输入 255.255.255.0。

**【问题 3】**设置最大连接数。具体操作步骤是：在 FTP 站点的属性窗口中切换到“FTP 站点”选项卡，选中“连接限制为”单选按钮，并在后面填入 100。

**【问题 4】**在 FTP 站点中，为每一个用户建立和用户名相同的虚拟目录，其真实路径指向该用户的主文件夹，并将权限设置为“读取”和“写入”。

# 2.4　Web 服务器配置

## 2.4.1　考点辅导

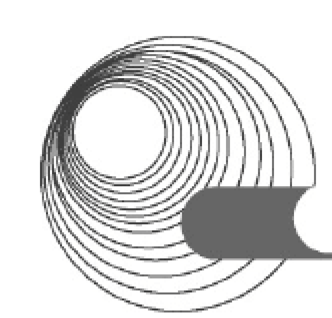
### 2.4.1.1　Windows 2008 R2 IIS 中 Web 服务器的配置

IIS 7.5 的 Web 服务组件安装成功后，就可以在这台服务器上创建 Web 站点了。默认情况下，在安装的过程中，系统会自动创建一个默认的 Web 站点。用户可以通过修改默认站点的属性发布自己的 Web 网站，也可以重新建立一个 Web 站点。

1. 网站的基本配置

通过“开始”→“管理工具”→“Internet 服务管理器”命令打开“Internet 信息服务(IIS)管理器”对话框。在管理器的左侧窗格中单击“网站”节点前的“+”号，然后选中某个希望配置的网站，右键单击该网站，在弹出的快捷菜单中选择“属性”命令，打开“属性”对话框。

在“网站”选项卡中可以设置网站的标识，包括网站描述、IP 地址和端口号，还可以设置连接超时、启用日志记录等，从网站日志记录中可以查看哪些用户访问了网站中的哪些内容，如图 2-30 所示。





在“主目录”选项卡中指定网站 Web 内容的来源，如图 2-31 所示。



图 2-30 “网站”选项卡

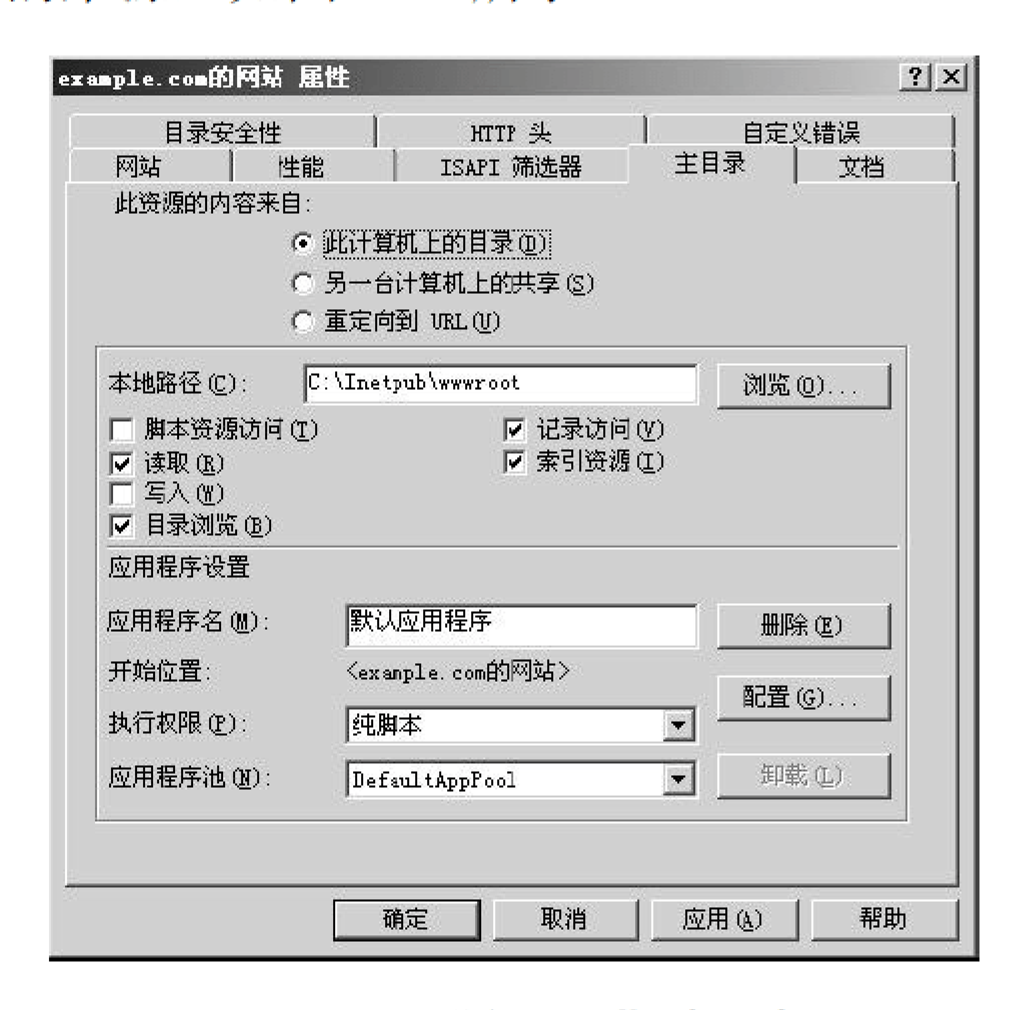


图 2-31 “主目录”选项卡

2. 网站的安全性配置

为了保证 Web 网站和服务器的安全，可以在“目录安全性”选项卡上为网站进行身份验证和访问控制、IP 地址和域名限制的设置，如图 2-32 所示。在“身份验证和访问控制”选项组中单击“编辑”按钮，打开如图 2-33 所示的“身份验证方法”对话框。使用该对话框可以配置 Web 服务器以验证用户身份。可以验证单个用户或选择用户组来阻止未授权用户与受限制内容建立 Web(HTTP)连接。

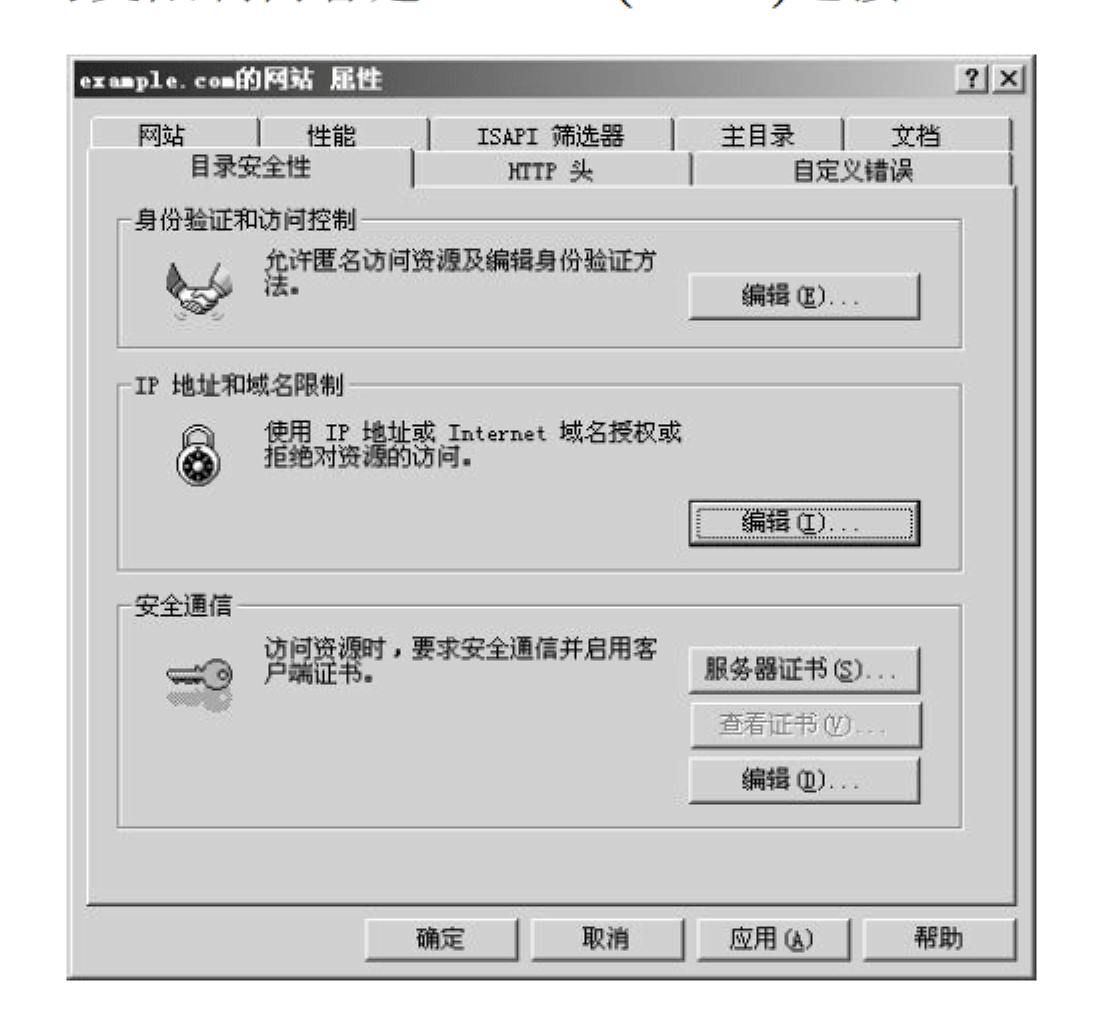


图 2-32 “目录安全性”选项卡

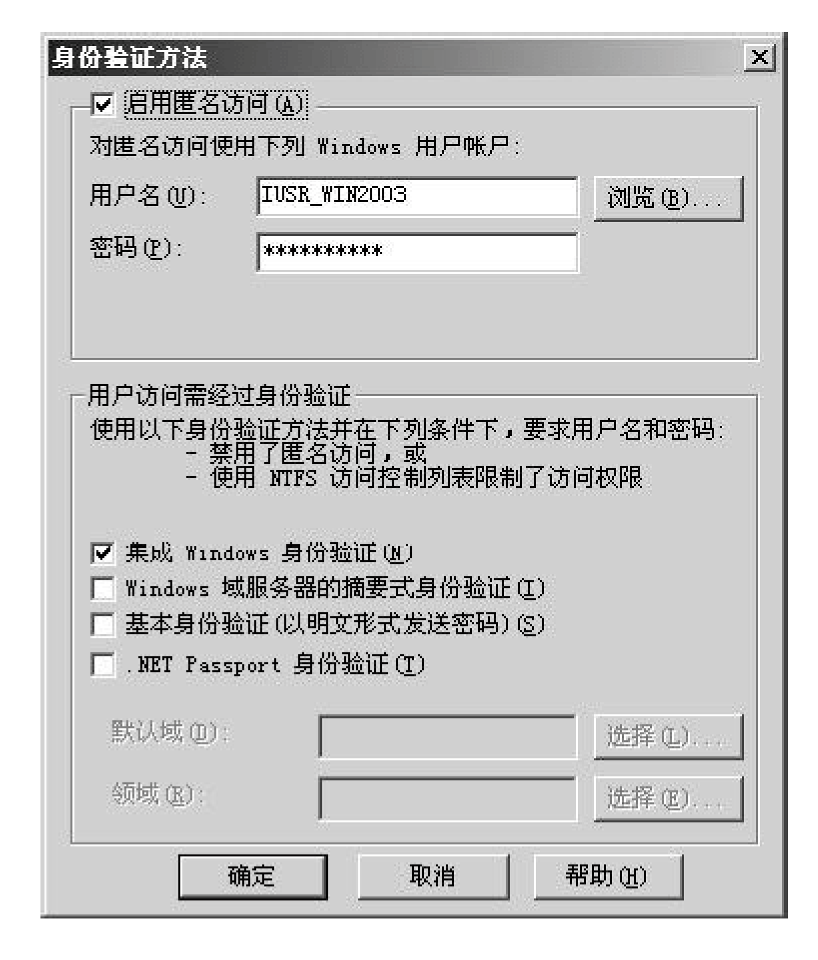


图 2-33 “身份验证方法”对话框

选中“启用匿名访问”复选框可以为用户建立匿名连接，此时用户无须专用的账户，而是使用匿名或来宾账户(Guest)登录到 IIS。默认情况下，服务器创建和使用账户 IUSR_计算机名，对应于本书所举的例子，用户名为 IUSR_WIN2008_R2。

如果用户希望对网站的访问者验证身份，也可以在“身份验证方法”对话框中的“用户访问需经过身份验证”选项组中进行设置。在此部分中选中的选项要求用户在访问服务

器上的任何信息前，提供有效的 Microsoft Windows 用户名和密码。当前 IIS 7.5 中提供了以下两种身份验证方法。

(1) 基本身份验证。用户使用基本身份验证访问 Web 站点时，系统会模仿为一个本地用户(即能实际登录到Web服务器的用户)登录到Web服务器，因此用于基本验证的Windows 用户必须具有“本地登录”用户权限。它是一种工业标准的验证方法，大多数浏览器支持这种验证方法。在使用基本身份验证方法时，用户密码是以未加密形式在网络上传输的，很容易被蓄意破坏系统安全的人在身份验证过程中使用协议分析程序破译用户和密码，因此这种验证方式是不安全的。

(2) 摘要式身份验证。摘要式身份验证也要求用户输入账号名称和密码，但账号名称和密码都经过 MD5 算法处理，然后将处理后产生的散列随机数(hash)传送给 Web 服务器。采用这种方法时，Web 服务器必须是 Windows 域的成员服务器。

(3) Windows 身份验证。集成 Windows 验证是一种安全的验证形式，它也需要用户输入用户账户和密码，但账户名和密码在通过网络发送前会经过散列处理，因此可以确保其安全性。Windows 身份验证方法有两种，分别是 Kerberos v5 验证和 NTLM，如果在 Windows 域控制器上安装了 Active Directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。

Windows 身份验证优先于基本身份验证，但它并不先提示用户输入用户名和密码，只有 Windows 身份验证失败后，浏览器才提示用户输入用户名和密码。虽然 Windows 身份验证非常安全，但是在通过 HTTP 代理连接时，Windows 身份验证不起作用，无法在代理服务器或其他防火墙应用程序后使用。因此，Windows 身份验证最适合企业 Intranet 环境。

用户可以基于 IP 地址或域名来允许或拒绝特定用户、计算机、计算机组或域访问该网站、目录或文件。在图 2-32 所示的“IP 地址和域名限制”选项组中单击“编辑”按钮，打开如图 2-34 所示的“IP 地址和域名限制”对话框。默认情况下，所有的计算机都被允许访问该网站。选中“授权访问”单选按钮，可以授权所有的计算机访问该网站，但在“下列除外”列表框中指定的计算机除外。要添加拒绝访问的计算机、计算机组或域，需单击“添加”按钮，打开如图 2-35 所示的“拒绝访问”对话框，在其中输入希望拒绝计算机的相应信息。输入后，单击“确定”按钮，被拒绝访问的计算机将出现在图 2-34 所示的“下列除外”列表框中。

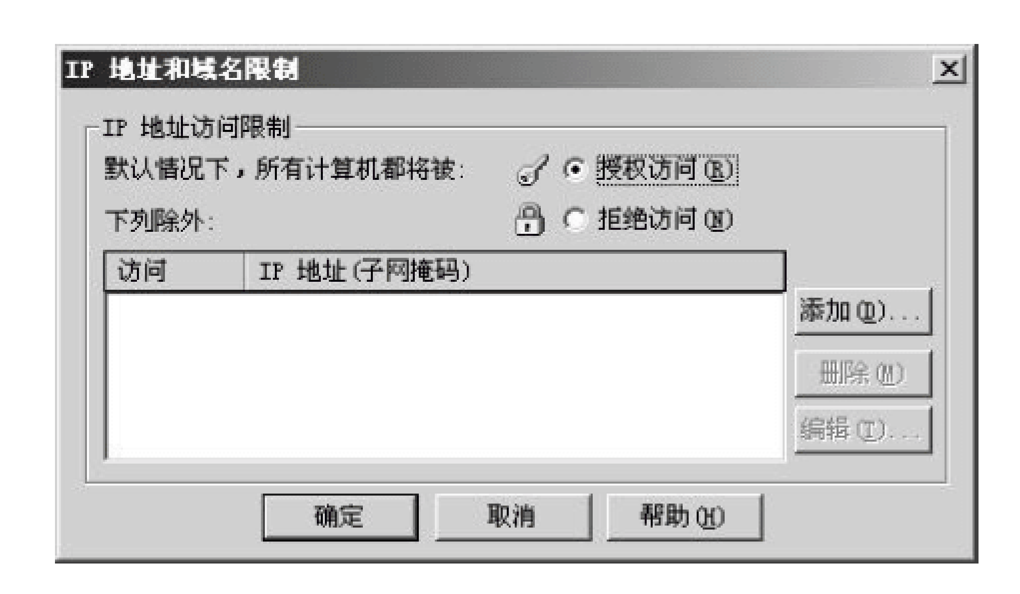



图 2-34　“IP 地址和域名限制”对话框




图 2-35　“拒绝访问”对话框

## 2.4.2　典型例题分析

**例 1**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2017

年 5 月下午试题二)

【说明】

某单位采用 Windows 操作系统配置 Web 服务器，根据配置回答下列问题。

【问题 1】(2 分)

图 2-36 是安装服务器角色界面截图，通过选中角色安装需要的网络服务。建立 FTP 需要选中__(1)__，创建和管理虚拟计算环境需要选中__(2)__，部署 VPN 服务需要选中__(3)__。




图 2-36　Windows 服务器配置截图

【问题 2】(4 分)

图 2-37 是 Web 服务安装后的网站管理界面，图中“MIME 类型”的作用是__(4)__。“SSL 设置”的作用是__(5)__，“错误页”的作用是__(6)__。

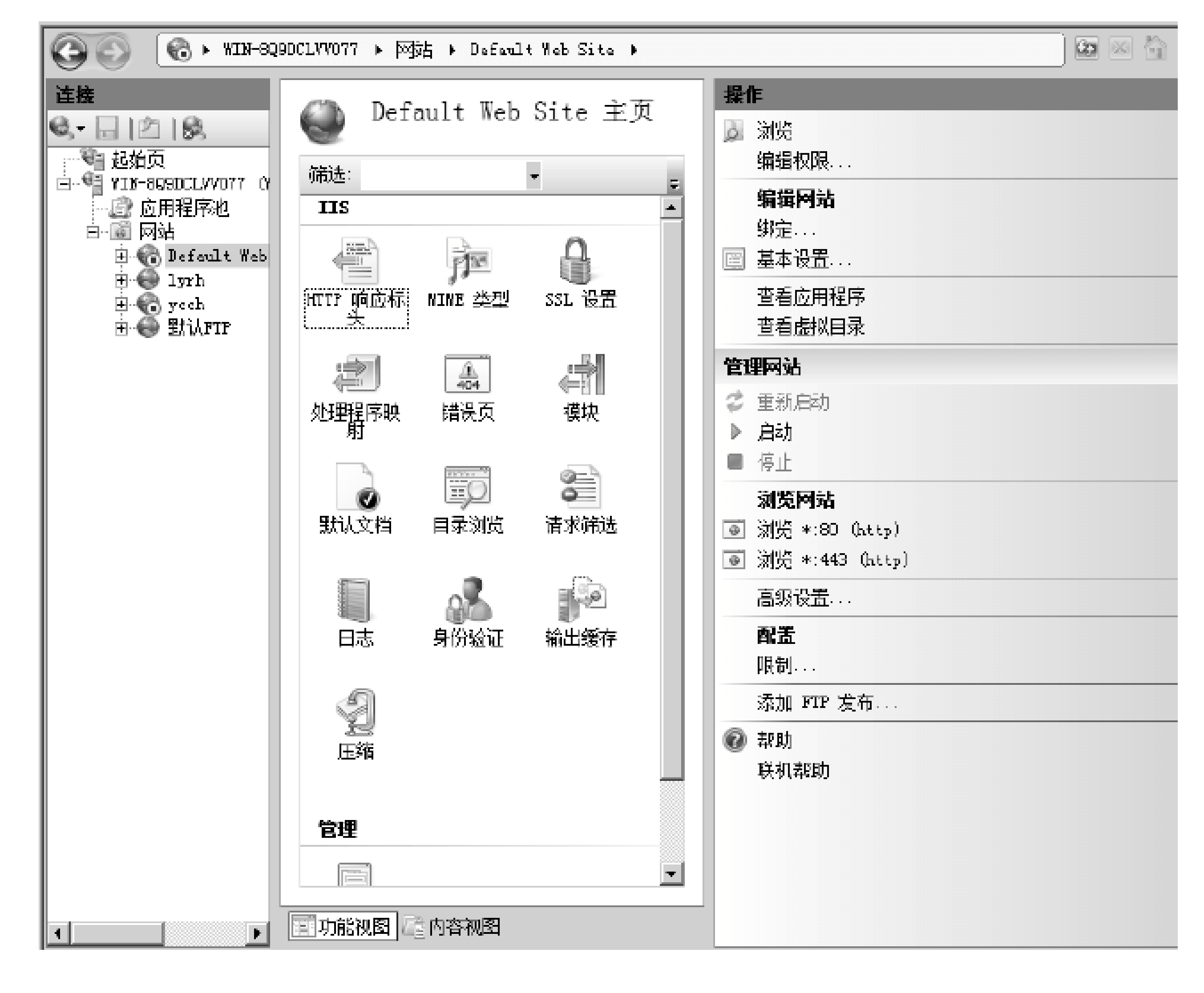



图 2-37　Web 服务器管理截图

(5)　备选答案：

A．配置网站 SSL 加密的 CA 证书路径　　B．配置网站或应用程序内容与 SSL 的关系

(6)　备选答案：

A．配置 HTTP 的错误响应　　　　　　　B．配置动态网页的错误

图 2-38 是配置添加网站的界面，图中“测试设置”的内容包括__(7)__和授权。采用图中配置，单击“确定”按钮后系统弹出的提示是__(8)__。

(8)　备选答案：

A．未配置主机名，确定以后再添加主机名。

B．端口已经分配，确定是否重复绑定端口。




图 2-38　Web 服务器配置图

【问题 3】

若该单位的防火墙做了服务器地址映射，则图 2-38 中“IP 地址”应填写为__(9)__。若服务器的域名是 www.test.com。“端口”更改为 8000，则外网用户访问该网站的 URL 是__(10)__。

(9)　备选答案：

A．给服务器分配的内网地址　　　　B．经过 DNS 解析的外网地址

**分析：**

【问题 1】

本题考查的是 Windows 操作系统配置 Web 服务器的基本知识与操作。

(1) 因为 Windows 操作系统中的 IIS 里内置了 FTP 模块，所以建立 FTP 需要选中 Web 服务器(IIS)。

(2) Hyper-V 是微软提出的一种系统管理程序虚拟化技术，能够实现桌面虚拟化，所以创建和管理虚拟计算环境需要选中 Hyper-V。

(3) 网络策略和访问服务，包括网络策略服务器(NPS)、健康注册机构(HRA)以及主机凭据授权协议(HCAP)的特定角色服务。可以使用 NPS 集中管理通过各种网络访问服务器(包括符合 RADIUS 标准的支持 802.1 X 的无线接入点、VPN 服务器、拨号服务器和支持 802.1 X 的以太网交换机)进行的网络访问。因此，部署 VPN 服务需要选中网络策略和访问服务。

**【问题 2】**

(4) MIME(Multipurpose Internet Mail Extensions)是描述消息内容类型的因特网标准。MIME 消息能包含文本、图像、音频、视频及其他应用程序专用的数据。因此，“MIME 类型”的作用是网站页面内可以包含图片、链接、甚至音乐、程序等非文字元素，使网站变得丰富多彩。

(5) 在图 2-37 中，“SSL 设置”的作用是配置网站 SSL 加密的 CA 证书路径。

(6) “错误页”的作用是配置 HTTP 的错误响应。

(7) 图 2-38 是配置添加网站的界面，图中“测试设置”的内容包括网页路径和授权。

(8) 从图 2-38 中可以看出主机没有配置，所以如果采用图中配置，单击“确定”按钮后系统弹出的提示是未配置主机名，确定以后再添加主机名。

**【问题 3】**

若该单位的防火墙做了服务器地址映射，则图 2-38 中“IP 地址”应填写为给服务器分配的内网地址。若服务器的域名是“www.test.com”端口更改为 8000，则外网用户访问该网站的 URL 是 http://www.test.com:8000。

**答案：**

**【问题 1】**

(1) Web 服务器(IIS)

(2) Hyper-V

(3) 网络策略和访问服务

**【问题 2】**

(4) 网站页面内可以包含图片、链接，甚至音乐、程序等非文字元素，使网站变得丰富多彩。

(5) A

(6) A

(7) 网页路径

(8) A

**【问题 3】**

(9) A

(10) http://www.test.com:8000

## 2.4.3 同步练习

1．阅读以下说明，回答问题 1～问题 6，将答案填入对应的答案栏内。

**【说明】**

某公司内部局域网连接方式如图 2-39 所示。某 Web 服务器 serverl 的域名为

www.goodweb.com。

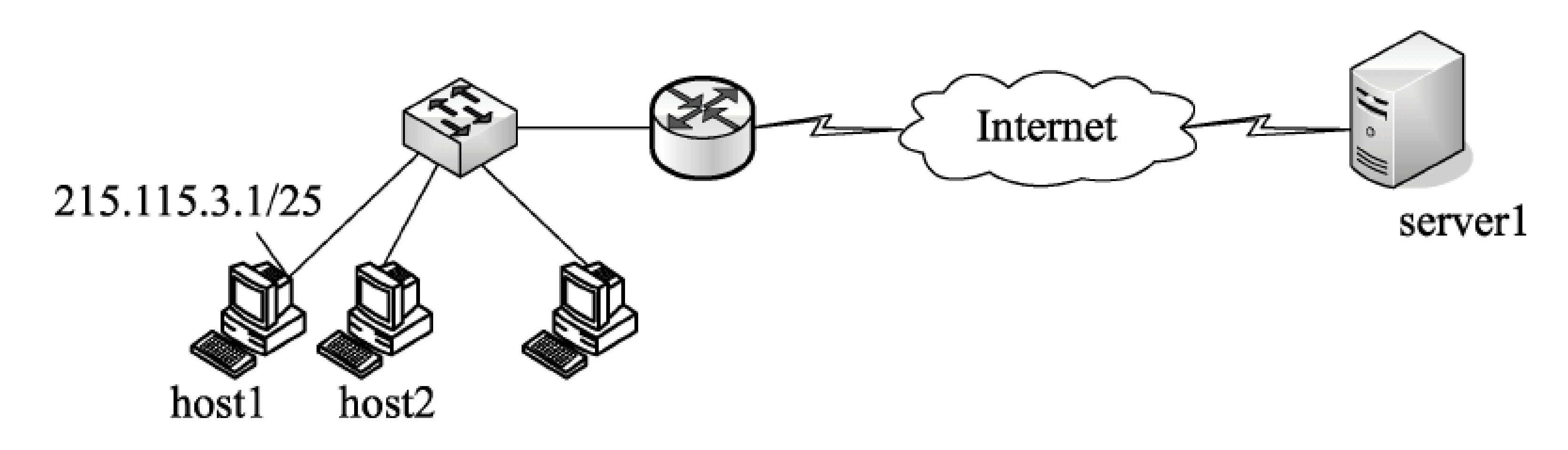



图 2-39

在主机 host1 的 Windows 命令行窗口输入 tracert www.goodweb.com 命令后，测试到 server1 所经过的连接情况如图 2-40 所示。

```
C:\Documents and Settings \wy>tracert www.goodweb.com
  1   <1 ms   <1 ms   <1 ms  215.115.3.2
  2   <1 ms   <1 ms   <1 ms  119.245.112.21
  3    *       *       *     Request timed out .
  4  3431 ms  3999 ms  4004 ms  192.270.255.201
  5   <1 ms   <1 ms   <1 ms  10.10.5.14
  6   <1 ms   <1 ms   <1 ms  102.117.1.13
Trace complete.
```

图 2-40

【问题 1】为 host2 配置 Internet 协议属性参数。

IP 地址：(范围) __(1)__；

子网掩码：__(2)__；

默认网关：__(3)__。

【问题 2】server1 的 IP 地址为__(4)__。

【问题 3】因公司业务发展，需要在该网段内新增一个 Web 站点对外提供服务，并通过防火墙来实现安全防范。防火墙可把其保护的区域分为内部网段和 DMZ 区，其中__(5)__的安全等级更高；新增的 Web 站点应放在防火墙的__(6)__。

【问题 4】公司内只有用户 host2 反映上网时断时续，采用命令__(7)__测试到网关的联通性，发现丢包严重；将交换机上连接 host1 和 host2 的接口互换，分别在两台计算机上测试到网关的联通性，此时发现 host2 正常，host1 丢包严重，则故障原因可能为__(8)__。

## 2.4.4　同步练习参考答案

1.

【问题 1】(1)　215.115.3.3～215.115.3.126

(2)　255.255.255.128

(3)　215.115.3.2

【问题 2】(4)　102.117.1.13

【问题 3】(5)　内部网段

(6)　DMZ

【问题 4】(7)　ping 或 ping215.115.3.2

(8)　交换机端口故障

# 2.5 DHCP 服务器配置

## 2.5.1 考点辅导

1. 安装 DHCP 服务器

Windows Server 2008 R2 系统内置了 DHCP 服务组件，但默认情况下并没有安装，需要管理员手动安装并配置，从而为网络提供 DHCP 服务。将一台运行 Windows Server 2008 R2 的计算机配置成 DHCP 服务器，最简单的方法是使用服务器管理器添加 DHCP 服务器角色，其过程如下：

(1) 通过“开始”菜单打开“服务器管理器”窗口，选择左侧的“角色”节点，单击“添加角色”超链接，启动添加角色向导。

(2) “开始之前”向导页中提示了此向导可以完成的工作，以及操作之前应注意的相关事项，单击“下一步”按钮继续。

(3) “选择服务器角色”向导页中显示了所有可以安装的服务器角色。如果角色前面的复选框没有被选中，则表示该网络服务尚未安装。如果已选中，则说明该服务已经安装。这里选中“DHCP 服务器”复选框，单击“下一步”按钮继续。

(4) “DHCP 服务器”向导页中对 DHCP 服务器的功能作了简要介绍，单击“下一步”按钮继续。

(5) 在“选择网络连接绑定”向导页中选择此 DHCP 服务器将用于向客户端提供服务的网络连接，单击“下一步”按钮继续，如图 2-41 所示。

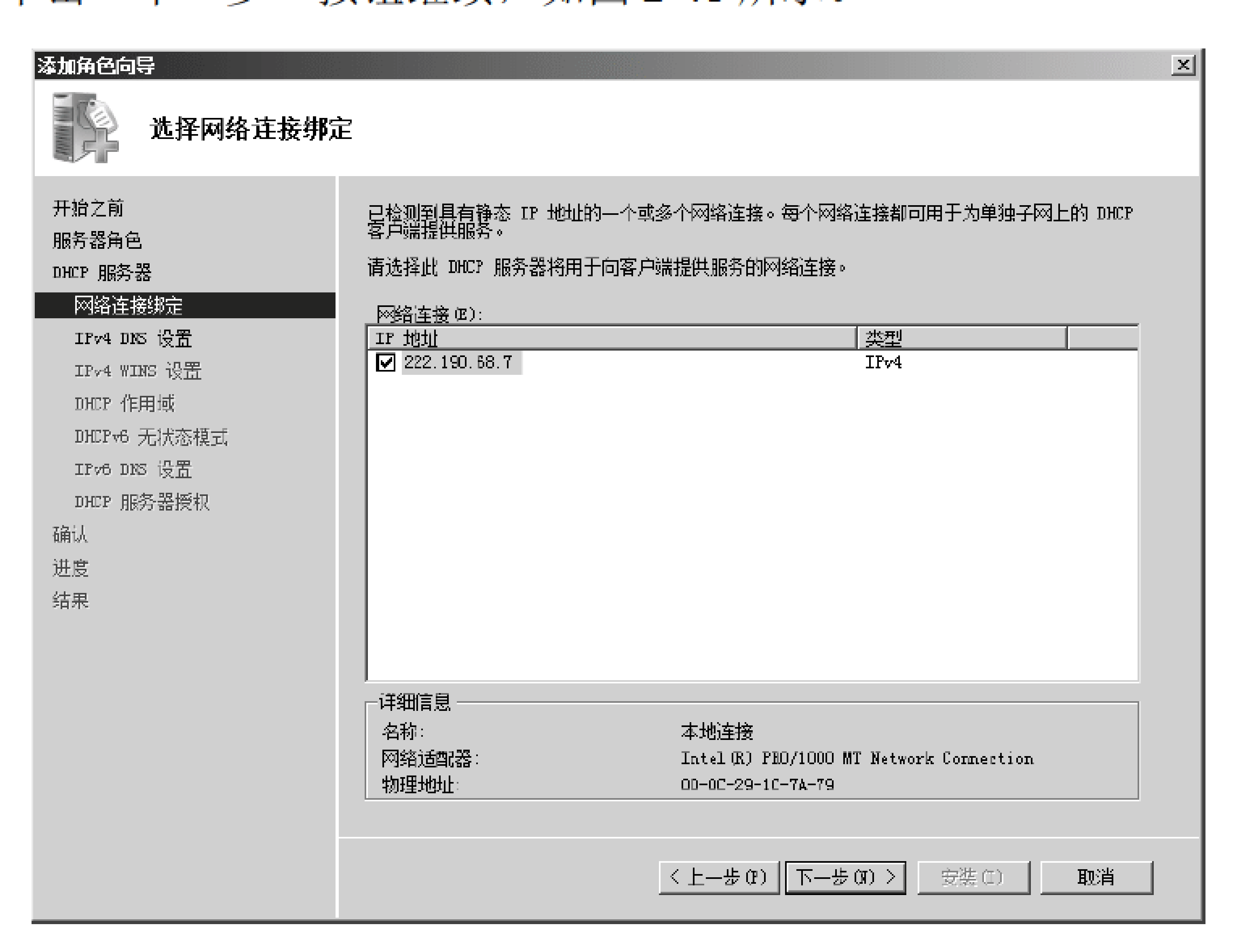



图 2-41 选择网络连接绑定

(6) 在“指定 IPv4 DNS 服务器设置”向导页中指定客户用于名称解析的父域名，以及

客户端用于域名解析的 DNS 服务器 IP 地址，单击“下一步”按钮继续，如图 2-42 所示。

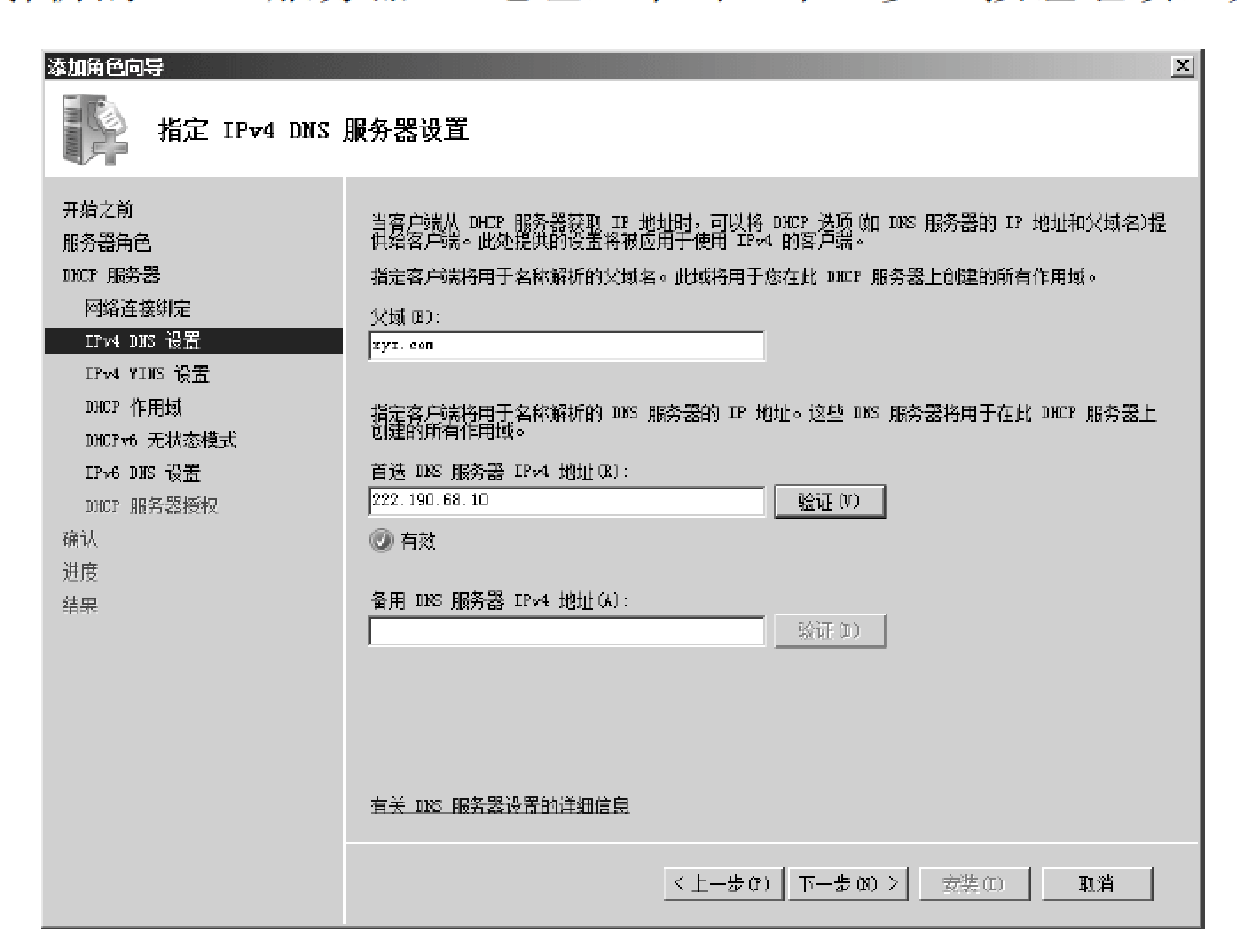



图 2-42　指定 IPv4 DNS 服务器设置

(7)　在“指定 IPv4 WINS 服务器设置”向导页中选择是否使用 WINS 服务，单击“下一步”按钮继续，如图 2-43 所示。

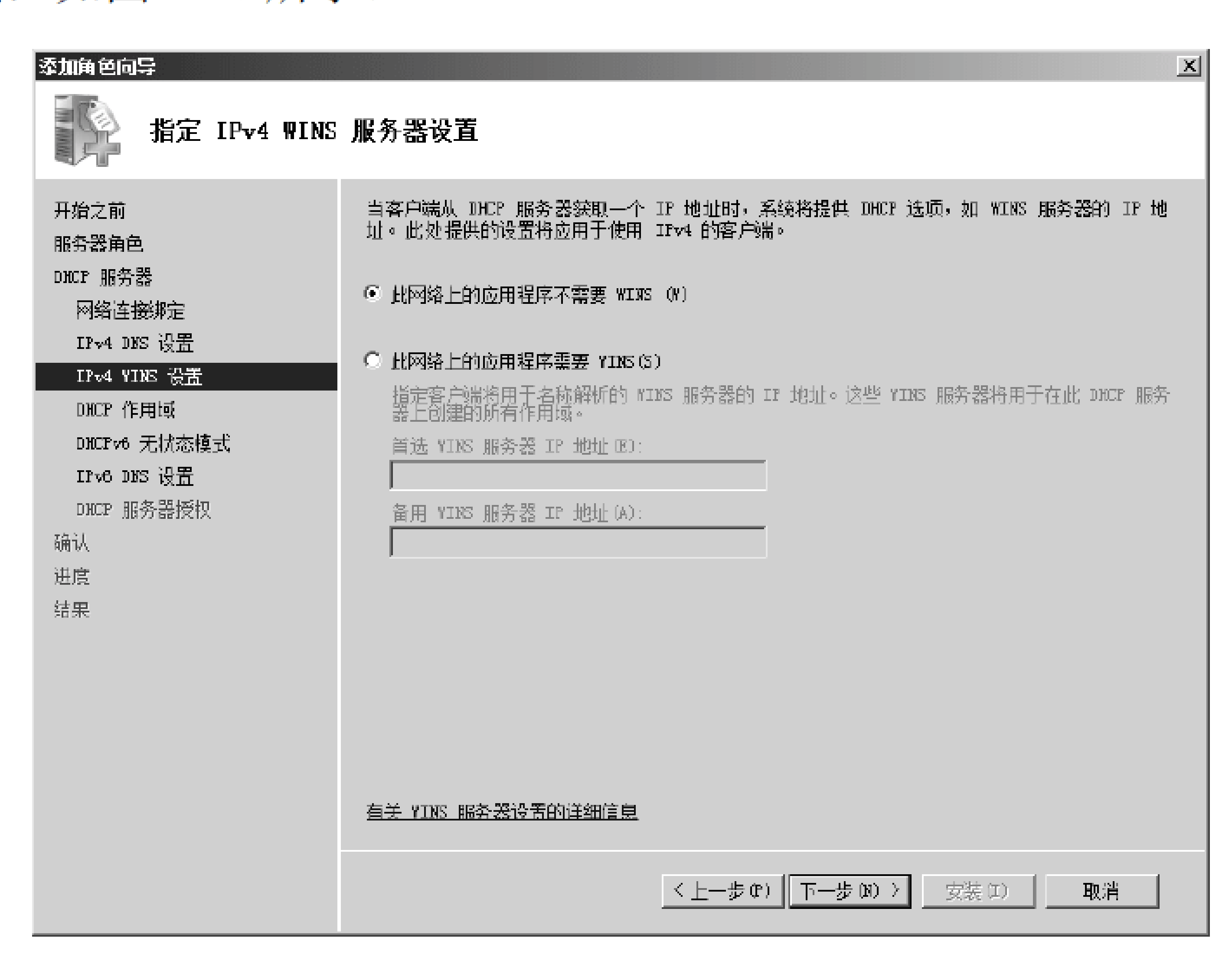



图 2-43　指定 IPv4 WINS 服务器设置

(8)　在“添加或编辑 DHCP 作用域”向导页中可以添加 DHCP 作用域。只有指定了作用域，DHCP 服务器才能向客户端分配 IP 地址、子网掩码和默认网关等。现在可以不指定，等 DHCP 安装完成后再添加。若现在指定，可单击“添加”按钮，如图 2-44 所示。

(9)　在“添加作用域”对话框中设置作用域的名称、起始 IP 地址、结束 IP 地址、子网掩码、默认网关以及子网类型。若选中“激活此作用域”复选框，则创建完成后会自动激活，如图 2-45 所示。设置完成后，单击“确定”按钮，返回上一步操作后单击“下一步”按钮继续。

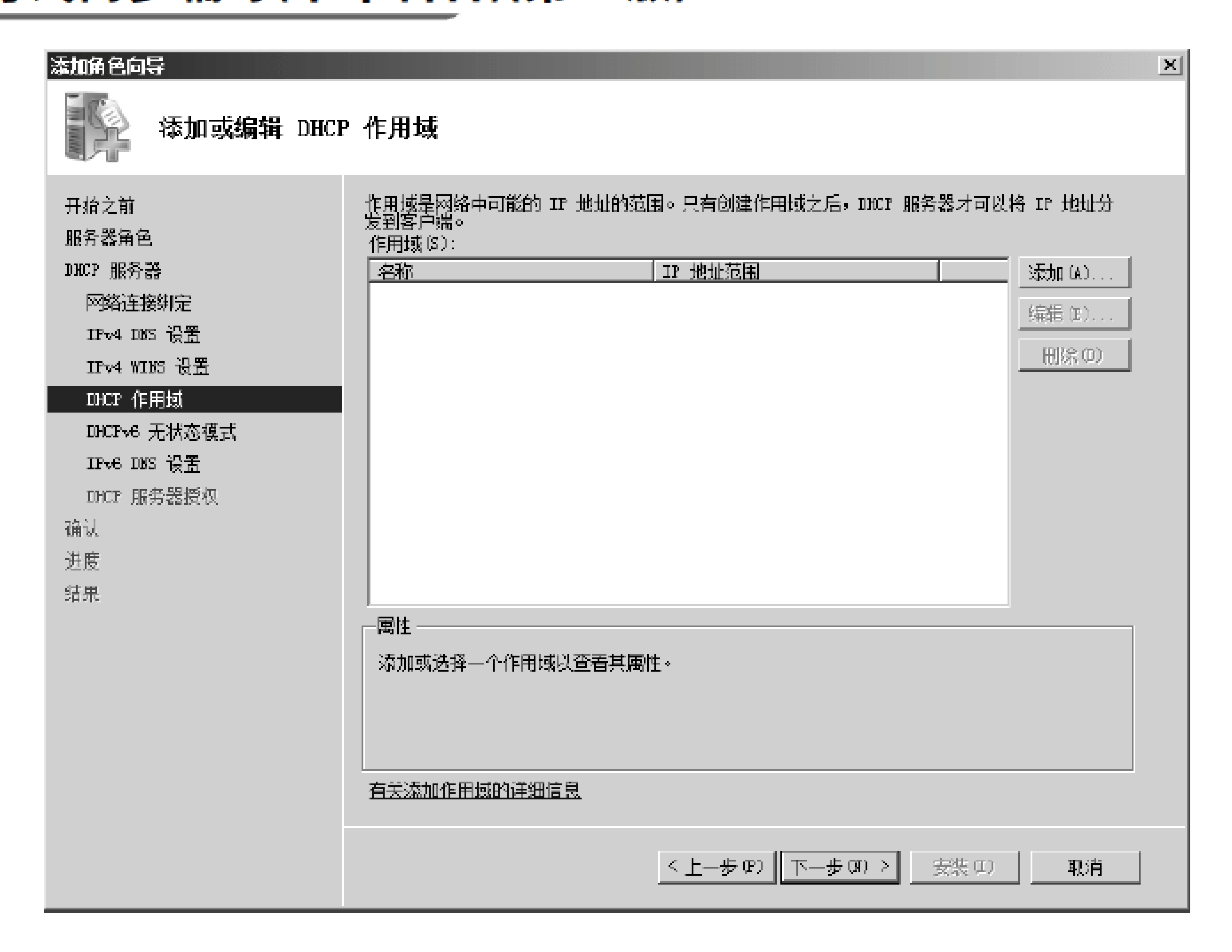



图 2-44　添加或编辑 DHCP 作用域

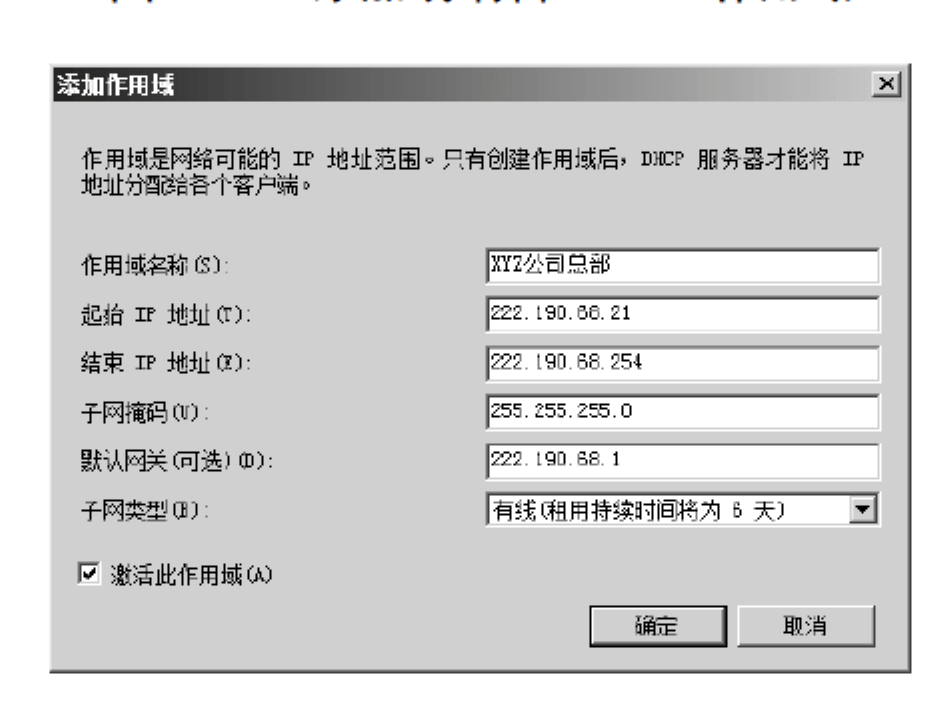



图 2-45　添加作用域

(10) 在“配置 DHCPv6 无状态模式”向导页中选择启用还是禁用服务器的 DHCPv6 无状态模式。选中“对此服务器禁用 DHCPv6 无状态模式”单选按钮，单击“下一步”按钮继续，如图 2-46 所示。

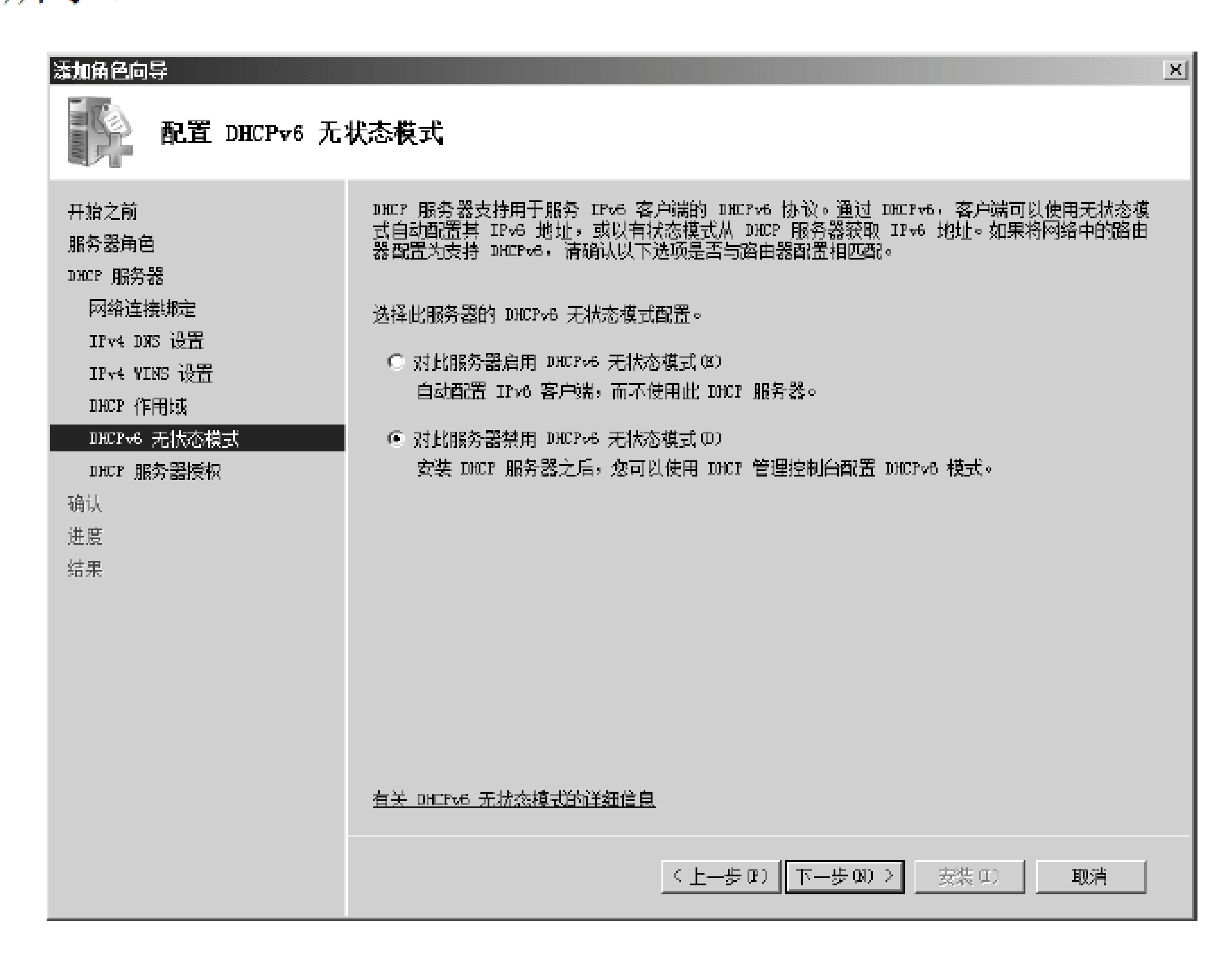



图 2-46　配置 DHCPv6 无状态模式

(11) 若 DHCP 服务器已加入了域，还会打开“授权 DHCP 服务器”向导页，若没有加入域，则不会出现此向导页。为 DHCP 服务器授权必须具有域管理员的权限，若当前没有以域管理员身份登录到域，则选中“使用备用凭据”单选按钮，然后单击“指定”按钮输入域管理员的用户名及密码。单击“下一步”按钮继续，如图 2-47 所示。

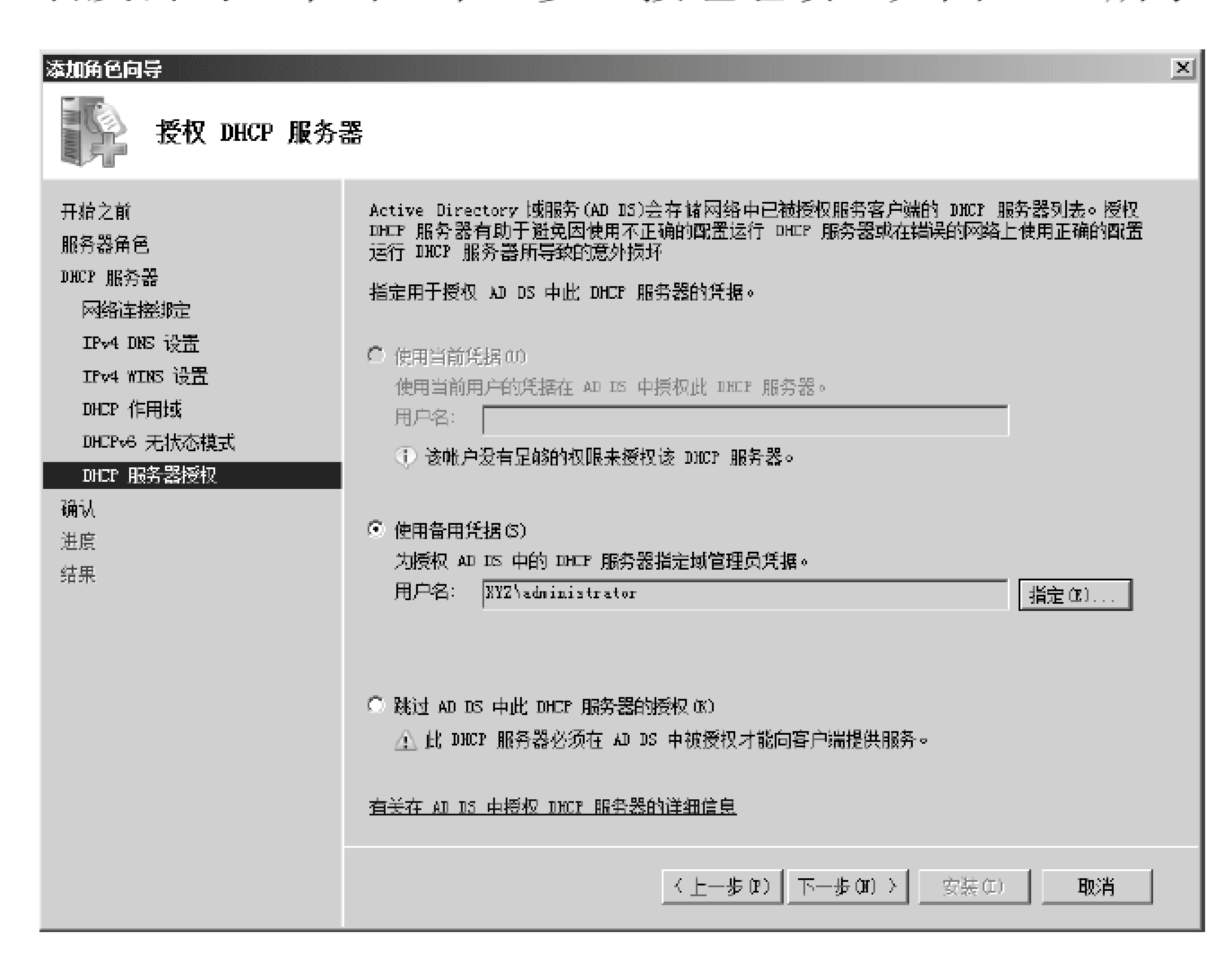



图 2-47　授权 DHCP 服务器

(12) 在“确认安装选择”向导页中，要求确认所要安装的服务器角色及配置情况，如果配置错误，可以单击“上一步”按钮返回。单击“安装”按钮即可开始安装 DHCP 服务器角色，如图 2-48 所示。

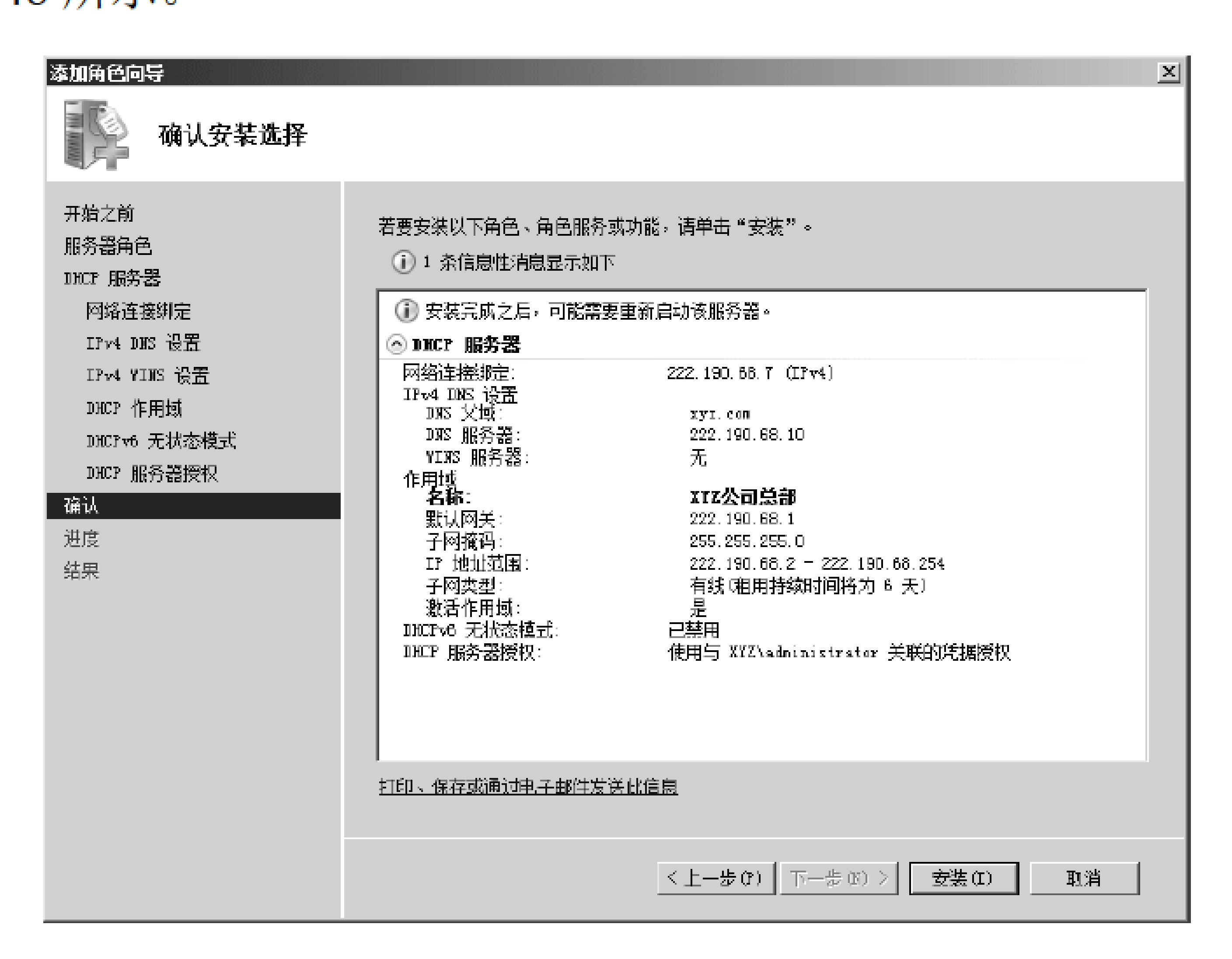



图 2-48　确认安装选择

(13) “安装进度”对话框中显示了安装 DHCP 服务器角色的进度，需耐心等待。

(14) “安装结果”对话框中显示 DHCP 服务器角色已经安装完成，提示用户可以使用 DHCP 管理器对 DHCP 服务器进行配置。若系统未启用 Windows 自动更新，还提醒用户设置 Windows 自动更新，以即时给系统打上补丁。单击“完成”按钮关闭添加角色向导便完

成了 DHCP 服务器的安装。

DHCP 服务器安装完毕后，可以通过选择“开始”→“管理工具”→DHCP 命令打开 DHCP 管理器，通过 DHCP 窗口可以管理本地或远程的 DHCP 服务器，如图 2-49 所示。

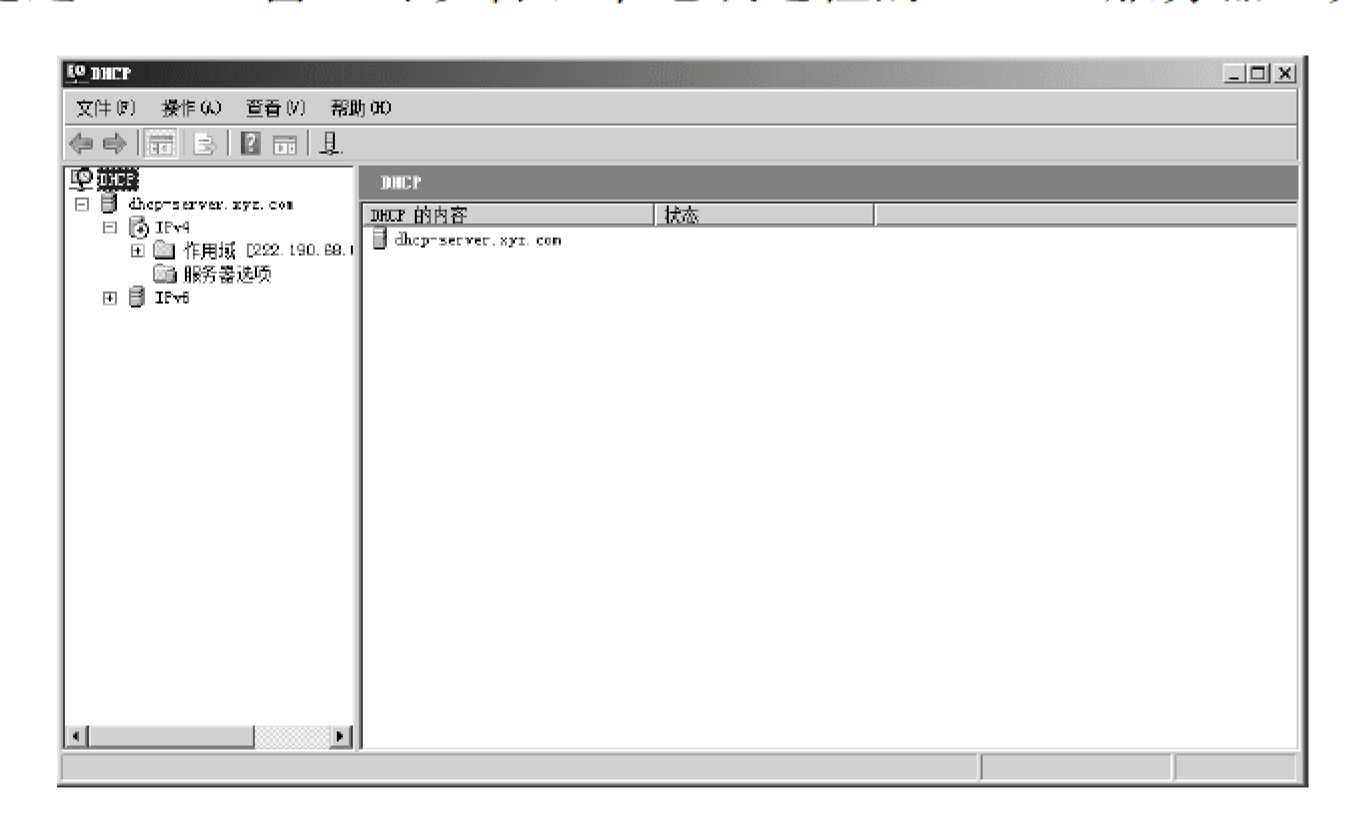


图 2-49　DHCP 管理器

2. 安装 DHCP 客户机

如果希望某台计算机能够自动获取 IP 地址，则需将这台计算机配置为 DHCP 客户机，配置方法如下。

(1) 在“控制面板”中单击“网络和 Internet 连接”图标，打开“网络和 Internet 连接”窗口。

(2) 在“网络和 Internet 连接”窗口中，单击“网络连接”图标，打开“网络连接”窗口。

(3) 右键单击“本地连接”图标，从弹出的快捷菜单中选择“属性”命令，选中“Internet 协议(TCP/IP)”，单击“属性”按钮，打开“Internet 协议(TCP/IP_)属性”对话框。

(4) 选中“自动获得 IP 地址”单选按钮，然后单击“确定”按钮，这样便把该计算机配置为 DHCP 客户机了。

3. 设置 DHCP 服务器

在安装了 DHCP 服务器之后，还需要在 DHCP 服务器上建立一个或多个 IP 地址作用域。“IP 地址作用域”是指可以分配给 DHCP 客户机的 IP 地址范围。这样，当 DHCP 客户机向 DHCP 服务器请求 IP 地址时，DHCP 服务器就可以从 IP 地址作用域中选择一个尚未被租用的 IP 地址，将其分配给 DHCP 客户机。

新建作用域的操作步骤如下。

(1) 依次执行“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。

(2) 在左侧窗格中，右键单击服务器名，在弹出的快捷菜单中选择“新建作用域”命令。

(3) 在弹出的“新建作用域向导”对话框中单击“下一步”按钮。

(4) 在“名称”文本框中输入一个能够清楚表示该作用域的名称，如图 2-50 所示。

(5) 单击“下一步”按钮，打开设置“IP 地址范围”的对话框。地址范围通过设置“起始 IP 地址”和“结束 IP 地址”来指定。通过设置“长度”，用户可以调整子网掩码，以指定 IP 地址中多少位作为网络 ID，多少位作为主机 ID，如图 2-51 所示。




图 2-50　设置作用域名

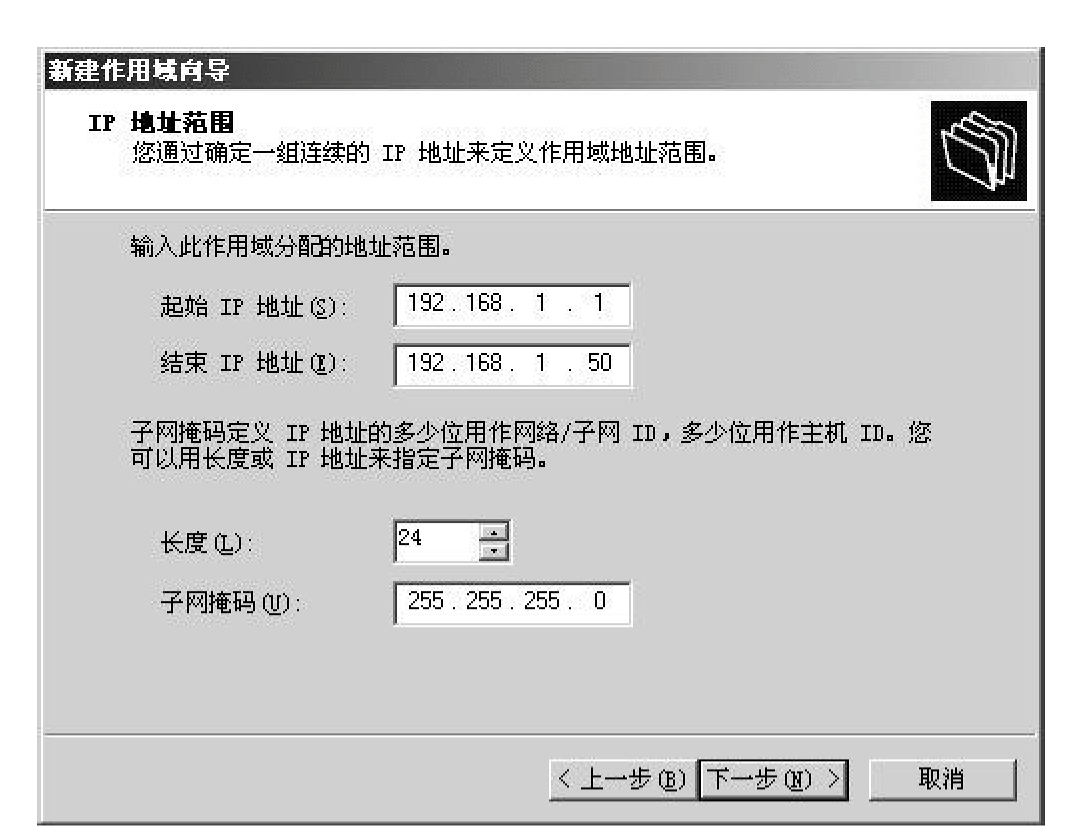



图 2-51　设置 IP 地址范围

(6) 设置好 IP 地址范围后，单击“下一步”按钮，打开“添加排除”对话框，如图 2-52 所示。这里用户可以指定前面设置的 IP 地址范围中有哪些地址不被服务器分配。如果想排除的 IP 地址是分散的，那么在“起始 IP 地址”中输入要排除的 IP 地址，然后单击“添加”按钮，重复这一过程直至所有要排除的 IP 地址均被添加。如果想排除的是某一段连续的 IP 地址，则分别输入该范围的起始 IP 地址和结束 IP 地址，然后单击“添加”按钮。

(7) 单击“下一步”按钮，打开“租约期限”对话框，如图 2-53 所示。租约期限指的是一个客户端从此作用域使用 IP 地址的时间长短。通常局域网使用的都是专用保留 IP 地址，地址数量很充裕，所以可以将租约期限设置得较长。

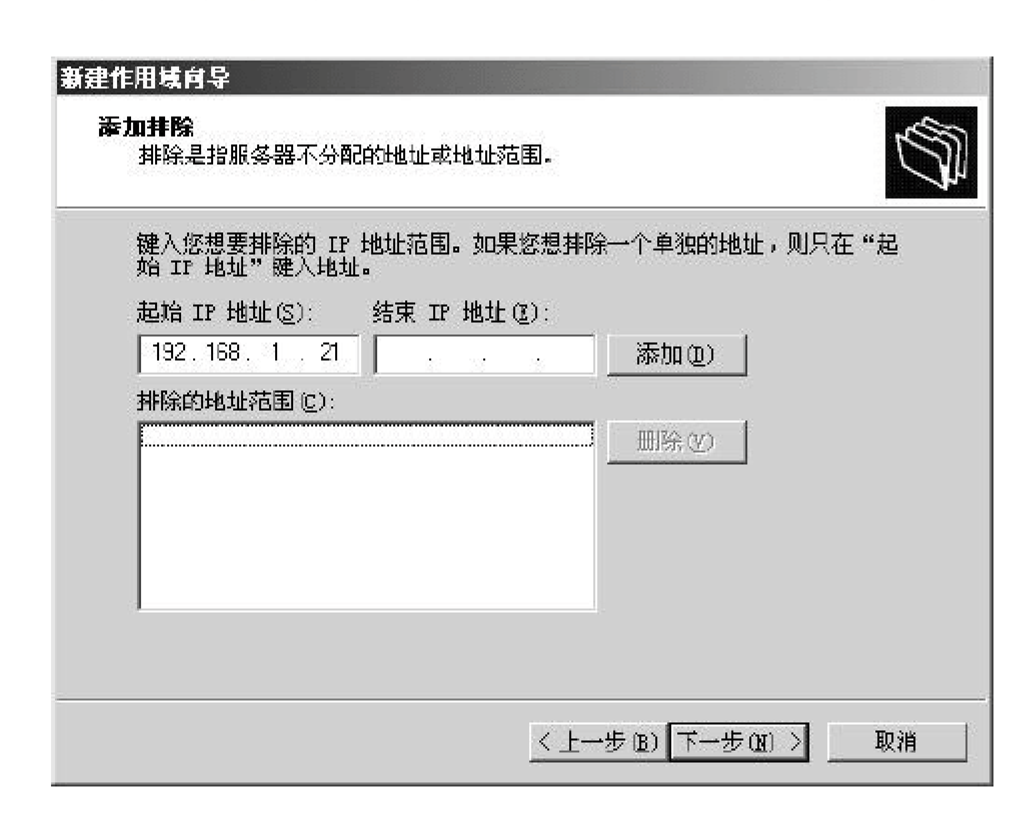



图 2-52　设置排除的 IP 地址

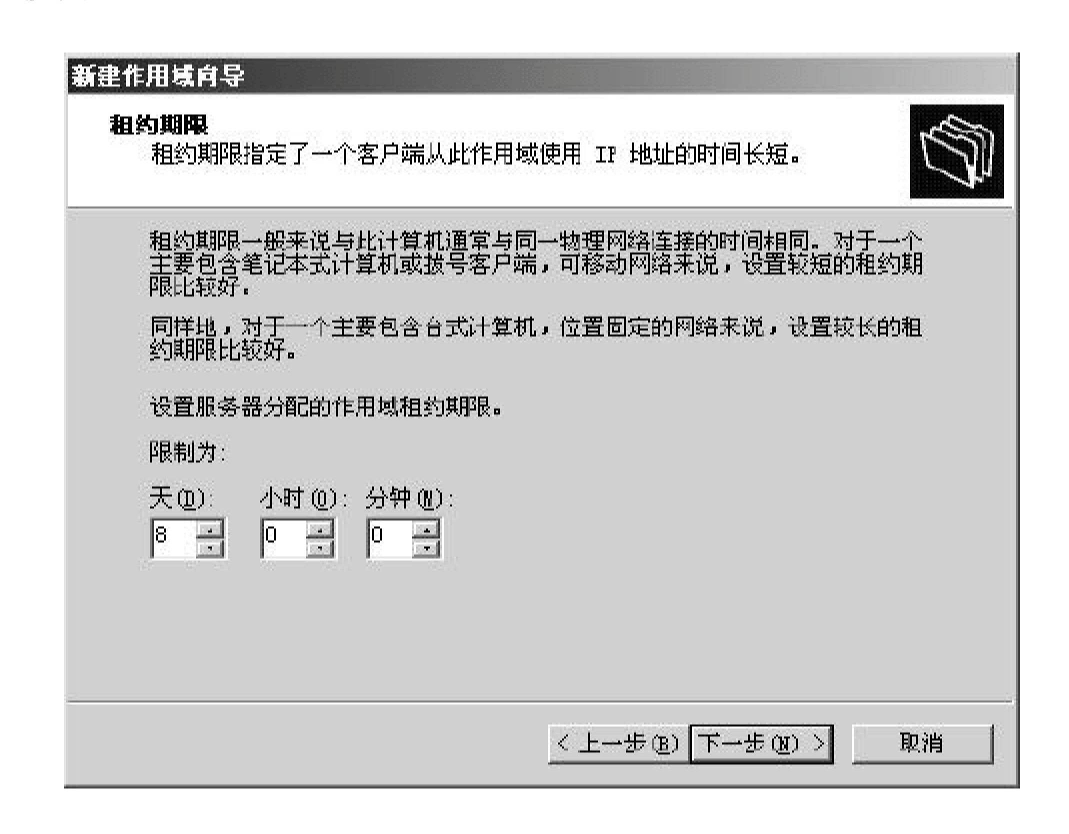



图 2-53　“租约期限”对话框

(8) 单击“下一步”按钮，向导提示用户为该作用域配置 DHCP 选项。通常只有正确配置了 DHCP 选项，DHCP 客户机才可以使用此作用域，所以选中“是，我想现在配置这些选项”单选按钮。

(9) 单击“下一步”按钮，首先要配置的是默认网关的 IP 地址。输入默认网关的 IP 地址，并单击“添加”按钮。

(10) 单击“下一步”按钮，接下来要配置的是域名称和 DNS 服务器。在“父域”文本框中输入域名，并在“IP 地址”文本框中输入 DNS 服务器的 IP 地址，然后单击“添加”按钮，如图 2-54 所示。若有多个 DNS 服务器，将其他的 DNS 服务器添加至此。通常设置两个 DNS 服务器即可，一个作为主 DNS 服务器，另一个作为辅 DNS 服务器。

(11) 单击“下一步”按钮，设置 WINS 服务器地址。如果网络中有 WINS 服务器，在“IP 地址”文本框中输入 WINS 服务器的地址，然后单击“添加”按钮，如图 2-55 所示。

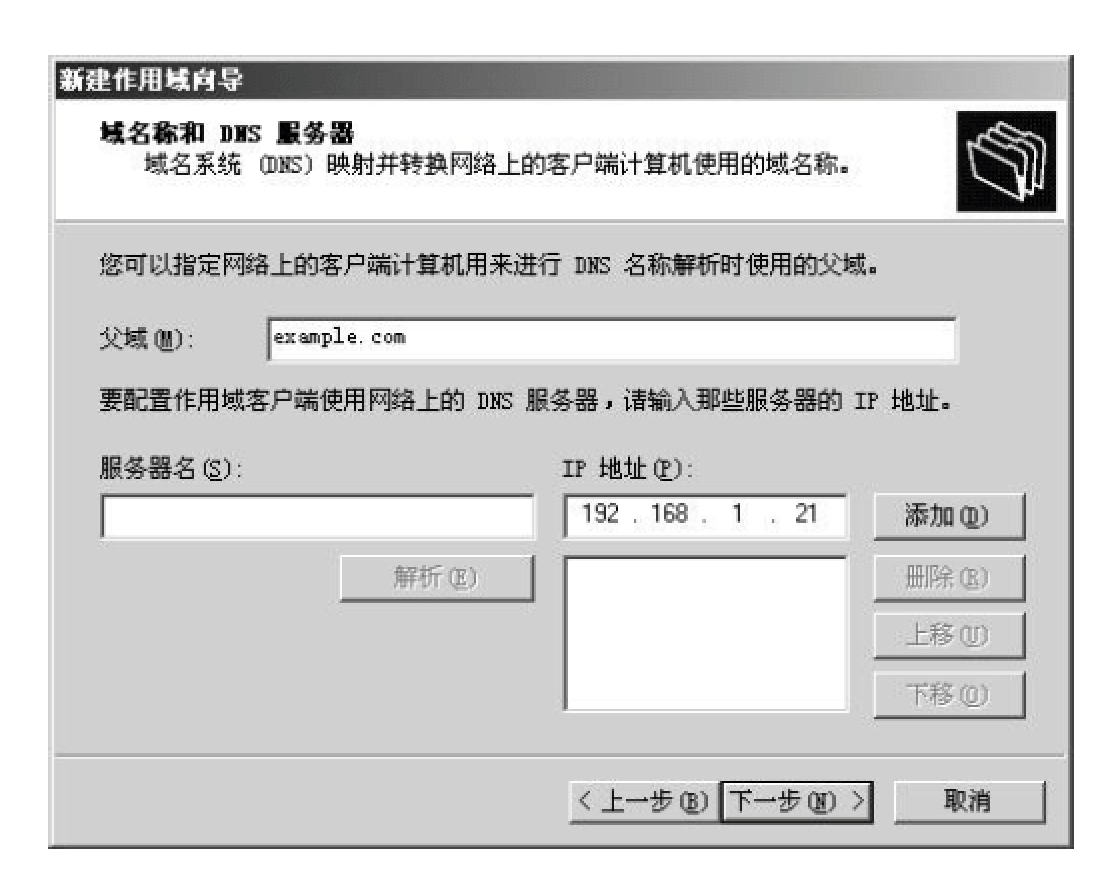



图 2-54　设置域名和 DNS 服务器

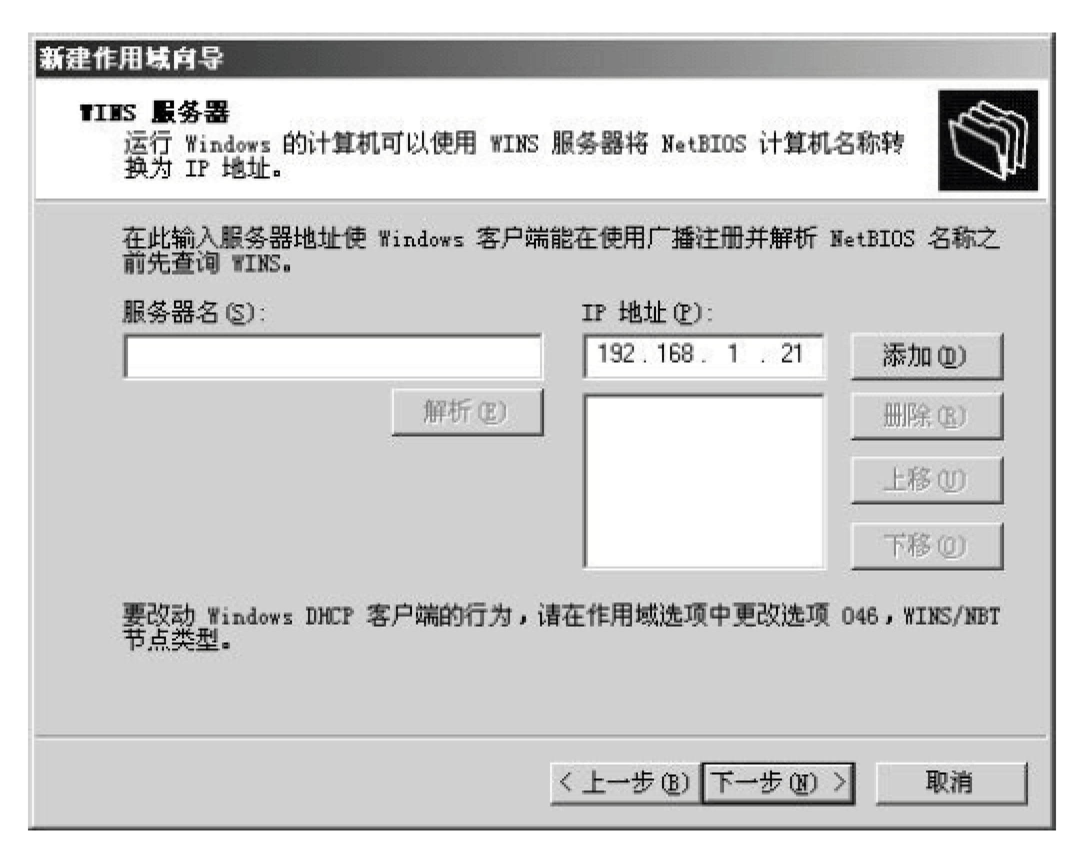



图 2-55　设置 WINS 服务器

(12) 单击“下一步”按钮，向导会提示是否激活此作用域，选择“是，我想现在激活此作用域”。

(13) 单击“下一步”按钮，向导提示已成功完成了新建作用域向导，单击“完成”按钮关闭向导。

接下来，系统会创建新的作用域。创建完成后的控制台如图 2-56 所示。展开新建的作用域，单击“地址池”选项，可以查看当前地址池中 IP 地址的范围及被排除的 IP 地址。单击“地址租约”选项，可以查看当前有哪些客户端租用了哪些 IP 地址。选择“保留”选项，可以查看并设置将地址池中的某些 IP 地址永久地分配给一些客户端。新建保留地址的方法是右键单击“保留”选项，在弹出的快捷菜单中选择“新建保留”命令，然后在弹出的对话框中输入相应的信息即可。需要注意的是，设置保留地址时，需要知道客户端网卡的 MAC 地址，即物理地址。网卡的物理地址可通过在“命令提示符”中运行 ipconfig /all 命令查看。

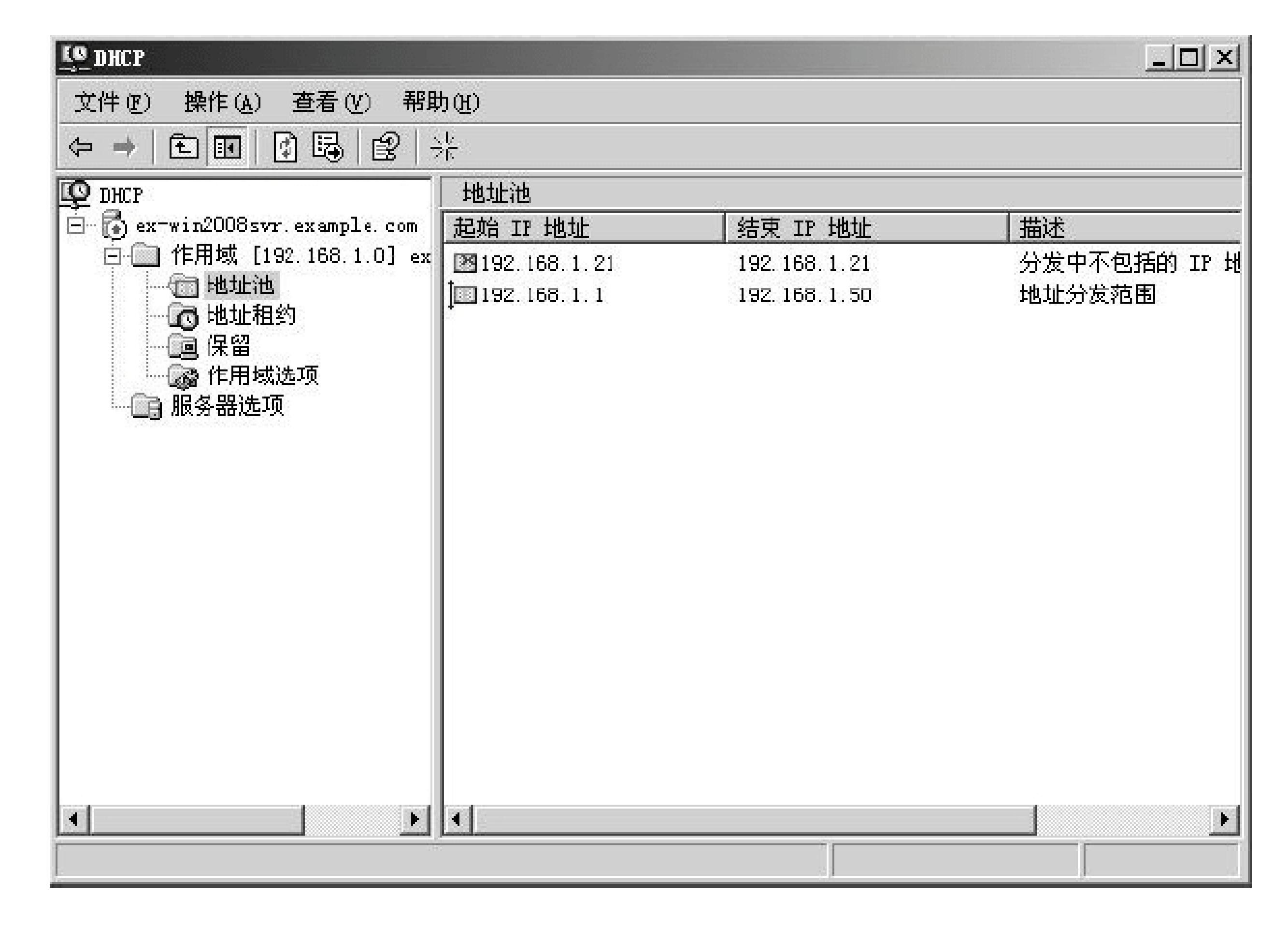



图 2-56　DHCP 服务器的地址池

单击“作用域 选项”选项，可以查看当前为该作用域设置的选项，也就是前面新建作用域向导中所设置的路由器、域名、DNS 服务器和 WINS 服务器等信息。这些是保证客户

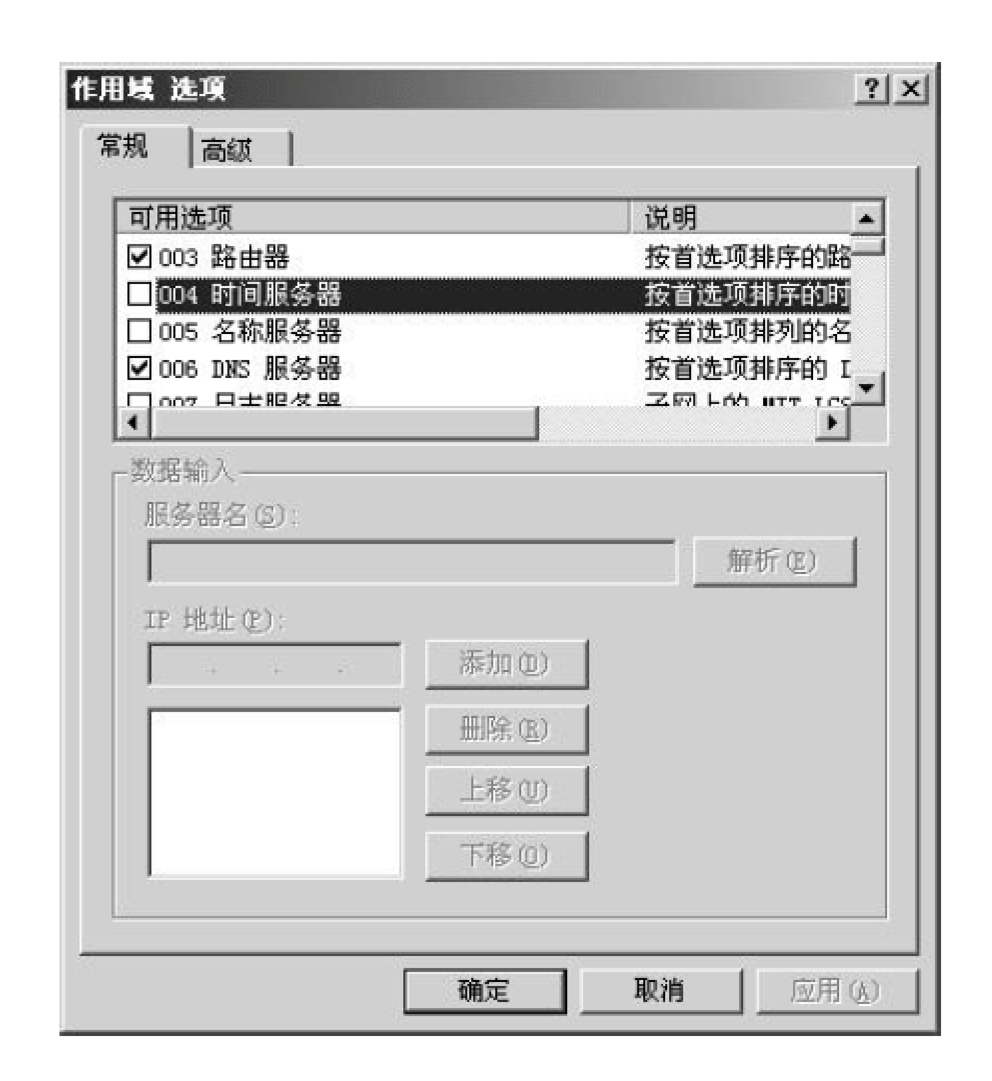
端能正常访问网络所必须的信息。如果用户还需要为该作用域设置其他的附加选项，可右击“作用域选项”，在弹出的快捷菜单中选择“配置选项”命令，如图 2-57 所示。打开如图 2-58 所示的“作用域 选项”对话框，在“可用选项”中选中要设置的选项，并在下面设置相应的信息，然后单击“确定”按钮即可。

右击新建的作用域，在弹出的快捷菜单中选择“属性”命令，可以对作用域的设置进行更改。作用域的属性对话框共有 3 个选项卡：“常规”、DNS 和“高级”选项卡。

“常规”选项卡如图 2-59 所示，在此可以更改作用域名、IP 地址范围和租约期限。




图 2-57　选择“作用域选项”→“配置选项”命令



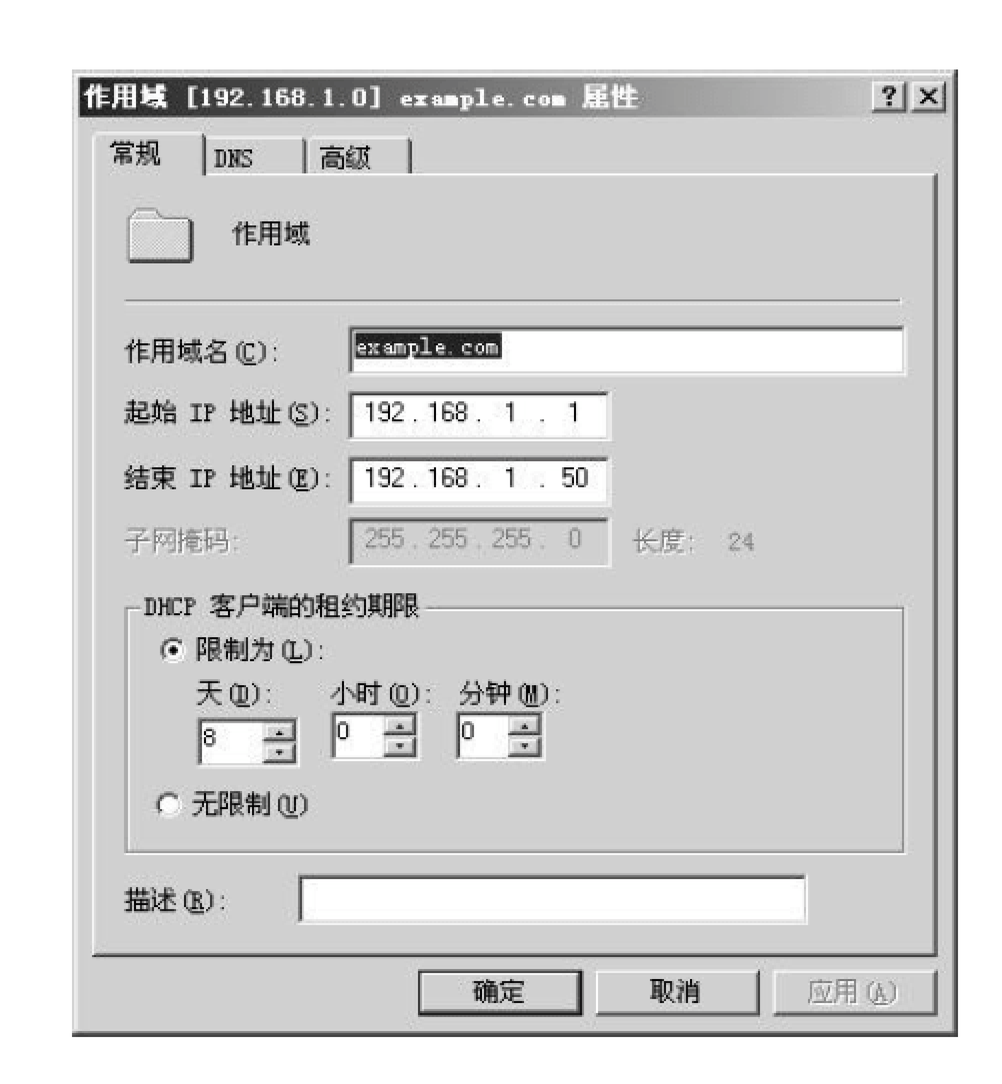





图 2-58　“作用域 选项”对话框

图 2-59　“常规”选项卡

DNS 选项卡可以设置 DHCP 服务器是否启用 DNS 动态更新。启用 DNS 动态更新的好处是当客户端的 IP 地址发生变化后，DHCP 服务器将会发送信息更新 DNS 服务器中该主机的主机和指针记录，以确保信息的一致性。

“高级”选项卡可以指定 DHCP 服务器为哪种类型的客户端动态分配 IP 地址，其中 BOOTP 一般为无盘工作站客户端，若网内没有无盘工作站，选择“仅 DHCP”选项即可。

当安装 DHCP 服务器的计算机同时也是域控制器时，在使用 DHCP 服务器前需对其进行授权，这是因为当错误配置或未授权的 DHCP 服务器被引入网络时，可能会引发问题。例如，如果启动了未授权的 DHCP 服务器，它可能会为客户端租用不正确的 IP 地址或者否认尝试续订当前地址租约的 DHCP 客户端。这两种配置中的任何一个都可能导致启用 DHCP 的客户端产生更多的问题。例如，从未授权的服务器获取配置租约的客户端将找不到有效的域控制器，从而导致客户端无法成功登录到网络。为了避免这些问题，在客户端之前运行 Windows Server 2008 R2 上的 DHCP 服务器服务时，需要验证是否已在 Active Directory 中对它们进行了授权。这样就避免了由于运行带有不正确配置的 DHCP 服务器或者在错误的网络上运行配置正确的服务器而导致的大多数意外破坏。DHCP 服务器一旦在授权列表中发现其 IP 地址，便进行初始化并开始为客户端提供 DHCP 服务。如果在授权列表中未发现自己的地址，则不进行初始化并停止提供 DHCP 服务。

授权的某台 DHCP 服务器的操作方法如下：依次选择“开始”→“管理工具”→DHCP 命令，打开 DHCP 管理控制台。右键单击要授权的服务器名，在弹出的快捷菜单中选择“授权”命令。授权过程需要一段时间，期间用户可以按 F5 键查看状态，检查是否完成授权。

要解除某台已授权服务器的授权，方法与授权过程相同，只是在弹出的快捷菜单中选择“撤销授权”命令即可。

## 2.5.2 典型例题分析

**例 1** 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2017 年 11 月下午试题二)

**【说明】**

某公司需要配置一台 DHCP 服务器，实现为用户分配指定范围的 E 地址、创建并置作用域、查看和更改租约等功能。

**【问题 1】**

在 DHCP 服务安装完毕后，需要获得__(1)__才可以响应客户的 IP 地址请求。

(1)备选答案：

A. 应答　　B. 授权

**【问题 2】**

DHCP 服务器为用户分配 E 地址，还可以为客户机分配__(2)__、__(3)__、__(4)__等 TCP/IP 协议属性参数。

**【问题 3】**

作用域是可以分配给子网中客户计算机的__(5)__范围。如果作用域是 192.168.1.101～192.168.1.105 和 192.168.1.109～192.168.1.110，比较简便的方法是在图 2-60 中将起始 IP 地址配置为__(6)__，结束 IP 地址配置为__(7)__，在图 2-61 中将起始 IP 地址配置为__(8)__，结束 IP 地址配置为__(9)__。

配置作用域时，除了配置 IP 地址外，还可配置其他属性参数，其中不包括__(10)__。

(10)备选答案：

A. DNS 服务器　　B. WINS 服务器　　C. DHCP 服务器　　D. 默认网关

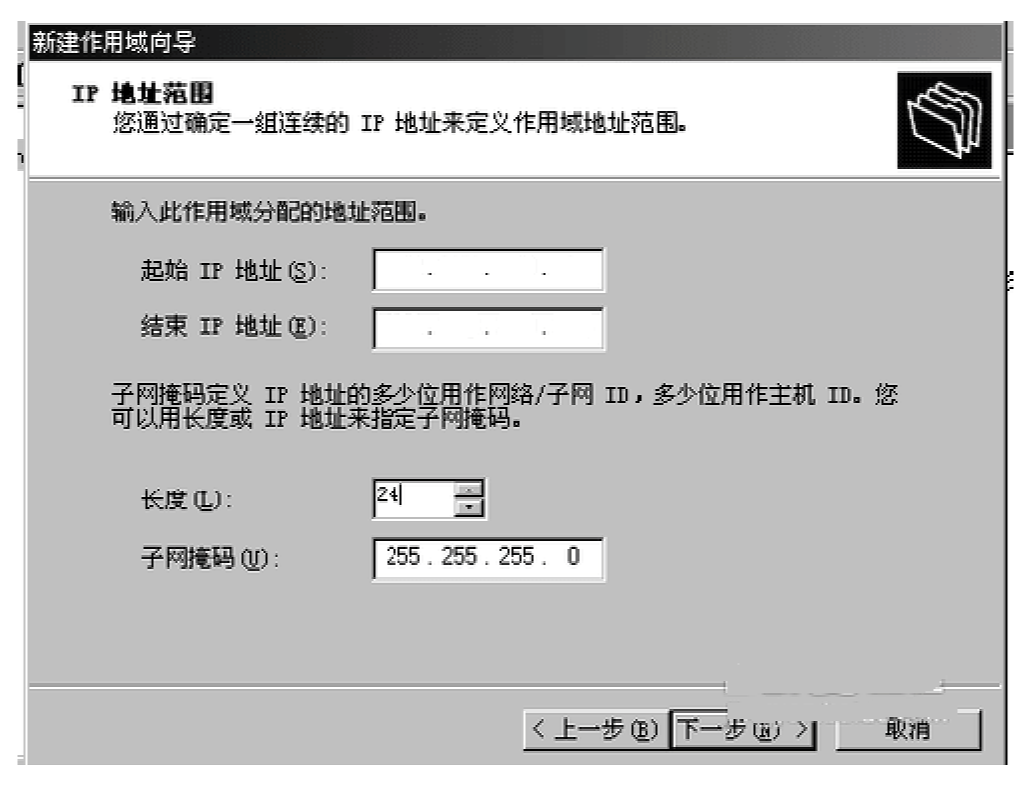





图 2-60 “IP 地址范围”界面

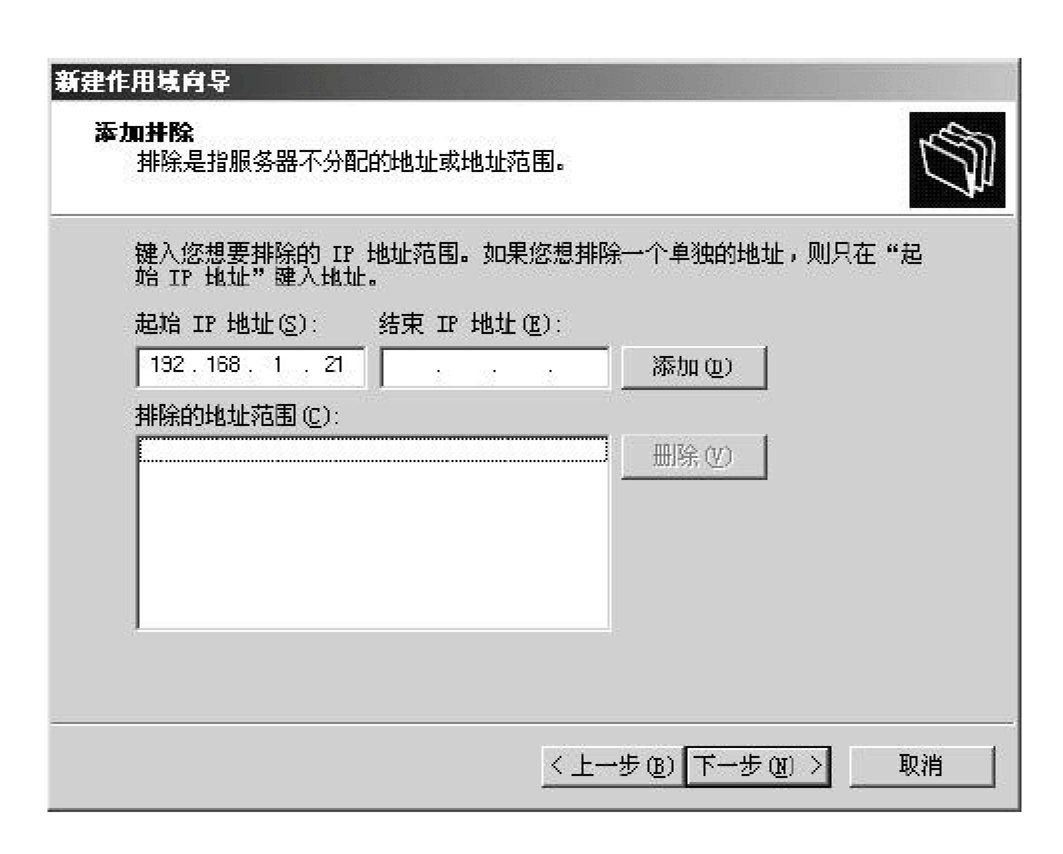



图 2-61 “添加排除”界面

**【问题 4】**

Windows 客户端会通过__(11)__的方式发送自动分配 IP 地址的请求文，经过与 DHCP 服务器的交互得到的 IP 地址，默认的 IP 地址租约期限是__(12)__天。在客户端使用 ipconfig/__(13)__命令可以释放租约，使用 ipconfig__(14)__命令重新向 DHCP 服务器申请地址租约，使用 ipconfig/__(15)__命令可查看当前地址租约等全部信息。根据图 2-62，DHCP 地址租约时长为__(16)__秒。

```
C:\>ipconfig /all

Windows IP Configuration

    Host Name ··············································: admin
    Primary Dns Suffix ·································:
    Node Type ···············································: Hybrid
    IP Routing Enable ·································: No
    WINS Proxy Enable ·································: No
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix ···············.:
    Description ············································: AMD PCNET Family PCI EthernetAdapter
    Physical Address ···································: 00-30-56-10-34-2E
DHCP Enable ···············································: Yes
Autoconfiguration Enable ························: Yes
IP Address ··················································: 192.168.1.102
Subnet Mask ················································: 255.255.255.0
Default Gateway ·········································: 192.168.1.1
DHCP Class ID ·············································: laptop
DHCPServer ·················································: 192.168.1.5
DNS Servers ·················································: 192.168.1.10
Primary WINS Server ··································: 192.168.1.5
Lease Obtained ············································: 2017 年 7 月 7 日  10:07:35
Lease Expires ··············································: 2017 年 7 月 7 日  11:07:35
```

图 2-62 地址租约信息

(13)～(15) 备选答案:

A. all　　B. renew　　C release　　D.setclassid

(16) 备选答案:

A. 1　　B. 60　　C .1800　　D.3600

**分析:**

本题考查 Windows 操作系统中 DHCP 服务器的配置情况。

**【问题 1】**

在 DHCP 服务安装完毕后，需要获得授权才可以响应客户的 IP 地址请求。

**【问题 2】**

DHCP 服务器为用户分配 IP 地址，还可以为客户机分配子网掩码、网关地址、DNS 服务器地址等 TCP/IP 协议属性参数。

**【问题 3】**

作用域是可以分配给子网中客户计算机的 IP 地址范围。如果作用域是 192.168.1.101～192.168.1.105 和 192.168.1.109~192.168.1.110，比较简便的方法是在图 2-61 中将“起始 IP”地址配置为 192.168.1.101，“结束 IP 地址”配置为 192.168.1.110，在图 2-62 中将“起始 IP 地址”配置为 192.168.1.106，“结束 IP 地址”配置为 192.168.1.108。

配置作用域时，除了配置 IP 地址外，还可以配置其他属性参数，其中不包括 DHCP 服务器。

**【问题 4】**

Windows 客户端会通过广播的方式发送自动分配 iP 地址的请求文，经过与 DHCP 服务器的交互得到的 IP 地址，默认的 IP 地址租约期限是 8 天。在客户端使用 ipconfig/ release 命令可以释放租约，使用 ipconfig renew 命令重新向 DHCP 服务器申请地址租约，使用 ipconfig/all 命令可查看当前地址租约等全部信息。根据图 2-63，DHCP 地址租约时长为 1 个小时，即 3600 秒。

总的参数简介(也可以在 DOS 方式下输入 ipconfig /? 进行参数查询)

- ipconfig /all: 显示本机 TCP/IP 配置的详细信息。
- ipconfig /release: DHCP 客户端手工释放 IP 地址。
- ipconfig /renew: DHCP 客户端手工向服务器刷新请求。
- ipconfig /flushdns: 清除本地 DNS 缓存内容。
- ipconfig /displaydns: 显示本地 DNS 内容。
- ipconfig /registerdns: DNS 客户端手工向服务器进行注册。
- ipconfig /showclassid: 显示网络适配器的 DHCP 类别信息。
- ipconfig /setclassid: 设置网络适配器的 DHCP 类别。
- ipconfig /renew “Local Area Connection”: 更新“本地连接”适配器的由 DHCP 分配 IP 地址的配置。
- ipconfig /showclassid Local*: 显示名称以 Local 开头的所有适配器的 DHCP 类别 ID。
- ipconfig /setclassid “Local Area Connection” TEST: 将“本地连接”适配器的 DHCP 类别 ID 设置为 TEST。

答案：

**【问题 1】**

(1) B

**【问题 2】**

(2) 子网掩码　　(3) 网关地址　　(4) DNS 服务器地址

**【问题 3】**

(5) IP 地址　　(6) 192.168.1.101　　(7) 192.168.1.110

(8) 192.168.1.106　　(9) 192.168.1.108　　(10) C

**【问题 4】**

(11) 广播　(12) 8　(13) C　(14) B　(15) A　(16) D

## 2.5.3　同步练习

1．阅读以下说明，回答问题 1～问题 5，将答案填入对应的解答栏内。

**【说明】**

某公司在国际网络互联中心申请了一个 C 类 IP 地址 210.45.12.0/24，域名为 abc.com.cn。该公司没有划分子网，使用一台 Cisco 2610 路由器接入互联网，其接入内部局域网的 IP 地址是 210.45.12.99，并有一台 DNS 服务器(210.45.12.10)、一台 Web 服务器(210.45.12.100)、一台 FTP 服务器(210.45.12.101)和一台 MAIL 服务器(210.45.12.102)。

原来该公司采用手工分配 IP 地址，现要改用 DHCP 自动分配 IP 地址，拟使用一台安装有 Windows Server 2008 R2 的 PC 服务器作为 DHCP 服务器，它的 IP 地址为 210.45.12.103。若你是该公司的网络管理员，需要配置这台 DHCP 服务器。假设该公司不会有新服务器，把所有的地址都动态地分配给客户机。

**【问题 1】**该作用域的 IP 地址范围是什么？子网掩码是多少？

**【问题 2】**排除范围是什么？

**【问题 3】**默认网关是什么？

**【问题 4】**域名是什么？域名服务器 IP 地址是什么？

**【问题 5】**该公司销售部有一台 PC，由于其工作性质决定了必须有一个固定 IP 地址，你如何给它分配一个固定 IP 地址？(写出两种方案)

## 2.5.4　同步练习参考答案

1．

**【问题 1】**该作用域的 IP 地址范围是 210.45.12.1～210.45.12.254；子网掩码为 255.255.255.0。

**【问题 2】**210.45.12.10、210.45.12.99～210.45.12.103。

**【问题 3】**210.45.12.99。

**【问题 4】**域名为 abc.com.cn 域名服务器 IP 地址是 210.45.12.10。

**【问题 5】**第一种方法是把要分配给该主机的 IP 地址加入排除范围之内；第二种方法是保留特定的地址，这时要输入保留名称、保留 IP 地址和该主机网卡的 MAC 地址。

## 2.6 本 章 小 结

本章知识点在 2009 年的新大纲中变化较小，主要删除了 Linux 环境下各种服务器的配置和维护。

本章知识点非常多，也是下午考试的重点之一。由于对应用服务器的配置是一个实践性很强的工作，考生在复习本章时应该尽可能亲手配置一下这些服务，这样印象会更深，学习起来能够理论联系实际，能更有效地掌握本章的知识。同时要注意配合《网络管理员考试同步辅导(计算机与网络基础知识篇)》第 5 章介绍的各种服务器基础知识一起学习。

本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目基本上涵盖了大纲规定的知识要点。

## 2.7 达标训练题及参考答案

### 2.7.1 达标训练题

1. 阅读以下说明，回答问题 1 至问题 3，将答案填入对应的答案栏内。

**【说明】**

某单位有一个网络，其中有一台主机的 IP 地址是 190.190.147.134。请回答以下问题。

**【问题 1】**这个地址是一个什么类型的地址？不划分子网时其网络地址是多少？广播地址是什么？

**【问题 2】**它的默认子网掩码是什么？

**【问题 3】**若子网掩码是 255.255.240.0，则这台主机所在的子网地址是什么？该子网的广播地址是什么？这个 IP 地址所在子网的主机 IP 范围是什么？

2. 阅读以下说明，回答问题 1 至问题 4，将解答填入对应的答案栏内。

**【说明】**

某公司申请了一个 C 类地址 196.102.56.0，公司有生产部门、市场部门、财务部门、人事部门、技术部门和经理办公室，每个部门都需要划分为单独的网络，即需要划分至少 5 个子网，每个子网至少支持 24 台主机。(使用固定子网掩码)

**【问题 1】**应将子网掩码设置为什么？

**【问题 2】**每个子网有多少个主机地址？

**【问题 3】**196.102.56.197 所在子网的网络地址是什么？

**【问题 4】**196.102.56.197 所在子网的广播地址是什么？

3. 阅读以下说明，回答问题 1 至问题 3，将解答填入对应的答案栏内。



**【说明】**

某一小型公司从 ISP 申请了一个 Internet 出口，ISP 给该公司提供了 5 个 IP 地址，分别是 222.34.109.66～222.34.109.70，ISP 给该公司提供的路由器地址是 222.34.109.65。

**【问题 1】**由于 ISP 忘记告诉子网掩码，你认为最有可能的子网掩码是什么？

**【问题 2】**这个子网的子网地址是什么？

**【问题 3】**这个子网有广播地址是什么？

4．阅读以下说明，回答问题 1 至问题 3，将答案填入对应的答案栏内。

**【说明】**

某公司被分配了一个 C 类地址 200.100.50.0，根据需要该公司将网络划分成若干个子网，其中：有 4 个子网，每个子网最多有主机 30 台；有 3 个子网，每个子网最多有主机 5 台；另外还有 9 个点到点串行链路。

**【问题 1】**请为该网络进行子网分割，至少有 3 个不同变长的子网掩码，并画出子网划分示意图。注意：该单位的路由器不支持全 0 和全 1 子网。

**【问题 2】**请列出你所分配的网络地址。

**【问题 3】**为该网络分配点到点串行链路地址。

5．阅读以下说明，回答问题 1 至问题 5，将解答填入对应的答案栏内。

**【说明】**

某公司使用了一台安装有 Linux 操作系统的 PC 服务器作为电子邮件服务器，邮件发送服务使用的是 sendmail 8.0。下面是 sendmail 的几个配置文件的片段：

/etc/sendmail.cf 文件片段：

```
Cwlocalhost
Fw/etc/mail/local-host-names
```

/etc/mail/access 文件内容：

```
localhost.localdomain        RELAY
localhost                    RELAY
127.0.0.1                    RELAY
210.45.45                    RELAY
aapla.edu.cn                 RELAY
       ____(1)____
```

/etc/aliases 文件内容：

```
bin:               root
daemon:            root
adm:               root
lp:                root
sync:              root
shutdown:          root
halt:              root
mail:              root
webmaster:         zhang
net_center:        zhang, taoan, liwenglong
owner-net_group: zhang
```

【问题 1】在/etc/sendmail.cf 文件中并未指定该电子邮件服务器的主机名，但它却能接收所有 abc.com.cn 域内的电子邮件，这个信息可能存放在哪儿？

【问题 2】该公司的员工最有可能在哪个网络中收发电子邮件？

【问题 3】在使用过程中，发现域 xyz.com.tw 上有人使用该服务器发送电子邮件，为了拒绝其访问，在(1)处该填写什么内容？

【问题 4】该公司主页上有一个电子邮件链接，邮件地址是 webmaster@abc.com.cn，单击它通过 Outlook Express 发送了一封电子邮件，该邮件将发送给谁？

【问题 5】命令#/usr/bin/makemap /etc/mail/access.db</etc/mail/access 的作用是什么？

6．阅读以下说明，回答问题 1 至问题 5，将解答填入对应的答案栏内。

【说明】

图 2-63 是某小型公司网络拓扑结构，其中代理服务器的两块网卡的设置已在图中标出。

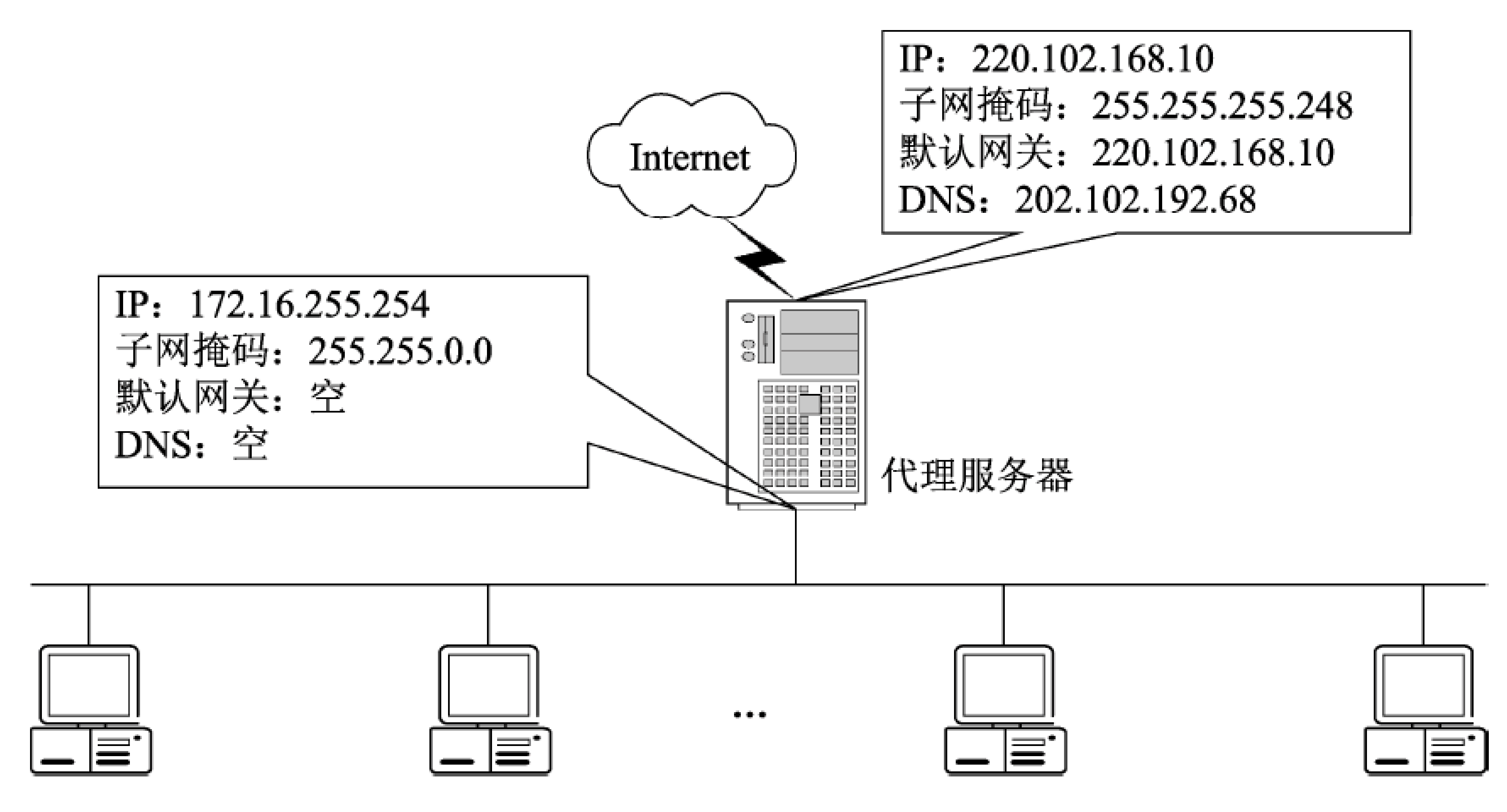



图 2-63　某小型公司网络拓扑结构

该代理服务器使用基于 Linux 的 Squid 代理服务器，下面为该服务器中文件/etc/squid/squid.conf 的一个片段。

```
http_port 8080
cache_mem 256 MB
cache_dir  /cache1 4000 24 33
cache_access_log /usr/local/squid/logs/access.log
cache_log /usr/local/squid/logs/cache.log
dns_nameservers ______(1)______
acl denydomain dstdomain foo.com.tw
acl all scr 0.0.0.0/0.0.0.0
http_access deny denydomain
http_access allow all
cache_mgr administrator@abc.com.cn
```

【问题 1】该公司主机的 IP 地址范围是什么？子网掩码是什么？

【问题 2】客户机的 IE 代理服务器端口号应设置为多少？(采用传统代理)

【问题 3】该代理服务器缓冲区放在哪里？大小是多少？能建多少一级目录、二级目录？

【问题 4】(1)处应填入什么内容？

【问题 5】文件中两行阴影语句的作用是什么？

7．某单位的网络要配置一台 DHCP 服务器，为网络内部的计算机自动分配 IP 地址。在考虑 DHCP 服务器时回答以下问题。

【问题 1】客户机启动时是如何从 DHCP 服务器得到动态 IP 的？

【问题 2】DHCP 客户机在启动时并没有 IP 地址，也不知道 DHCP 服务器的地址，那么它与 DHCP 服务器之间是通过什么方式进行通信的？

【问题 3】配置 DHCP 服务器应具备什么条件？

【问题 4】Windows 2000 用户通过什么命令可以看到自己租约到的本机 IP 地址？用何命令可以重新向 DHCP 服务器租约 IP？用何命令可以释放 IP？

8．阅读以下说明，回答问题 1 至问题 5，将解答填入对应的答案栏内。

**【说明】**

在 Linux 下安装、配置 Apache 服务，Apache 服务程序 httpd 启动时需要读取配置文件 httpd.conf。以下是 httpd.conf 配置文件的一个片段：

```
## httpd.conf -- Apache HTTP server configuration file
### Section 1: Global Environment
ServerType standalone
ServerRoot "/etc/httpd"
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MaxClients 150
### Section 2: 'Main' server configuration
Port 80
User apache
Group apache
ServerAdmin webmaster@abc.com.cn
ServerName www.abc.com.cn
DocumentRoot "/var/www/html"
UserDir public_html
DirectoryIndex index.html
Alias /jianji "/home/zhang/jianji"
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
ErrorDocument 404 /missing.html
### Section 3: Virtual Hosts
NameVirtualHost 192.168.10.101
<VirtualHost 192.168.10.101>
   ServerAdmin webmaster@abc.com.cn
   DocumentRoot /www/htdocs/abc
   ServerName markert.abc.com.cn
   ErrorLog logs/host.some_domain.com-error_log
   CustomLog logs/host.some_domain.com-access_log common
</VirtualHost>
```

【问题 1】该 Web 服务器的工作目录是什么？

【问题 2】当用户要访问该 Web 服务器的一个文件时，这个文件已经被删除了，服务器该如何响应客户？

【问题 3】httpd.conf 文件中阴影部分语句的作用是什么？

【问题 4】当用户在浏览器中输入 http:// 192.168.10.100/zhang/时，将访问什么内容？

【问题 5】停止 Apache 服务器的命令是什么？

## 2.7.2 参考答案

1.

【问题 1】B 类地址、190.190.0.0、190.190.255.255

【问题 2】255.255.0.0

【问题 3】190.190.144.0、190.190.159.255、190.190.144.1～190.190.159.254

2.

【问题 1】255.255.255.224

【问题 2】30

【问题 3】196.102.56.192

【问题 4】196.102.56.223

3.

【问题 1】255.255.255.248

【问题 2】222.34.109.64

【问题 3】222.34.109.71

4.

【问题 1】255.255.255.224、255.255.255.248 和 255.255.255.252；图 2-64 是一种划分方法。

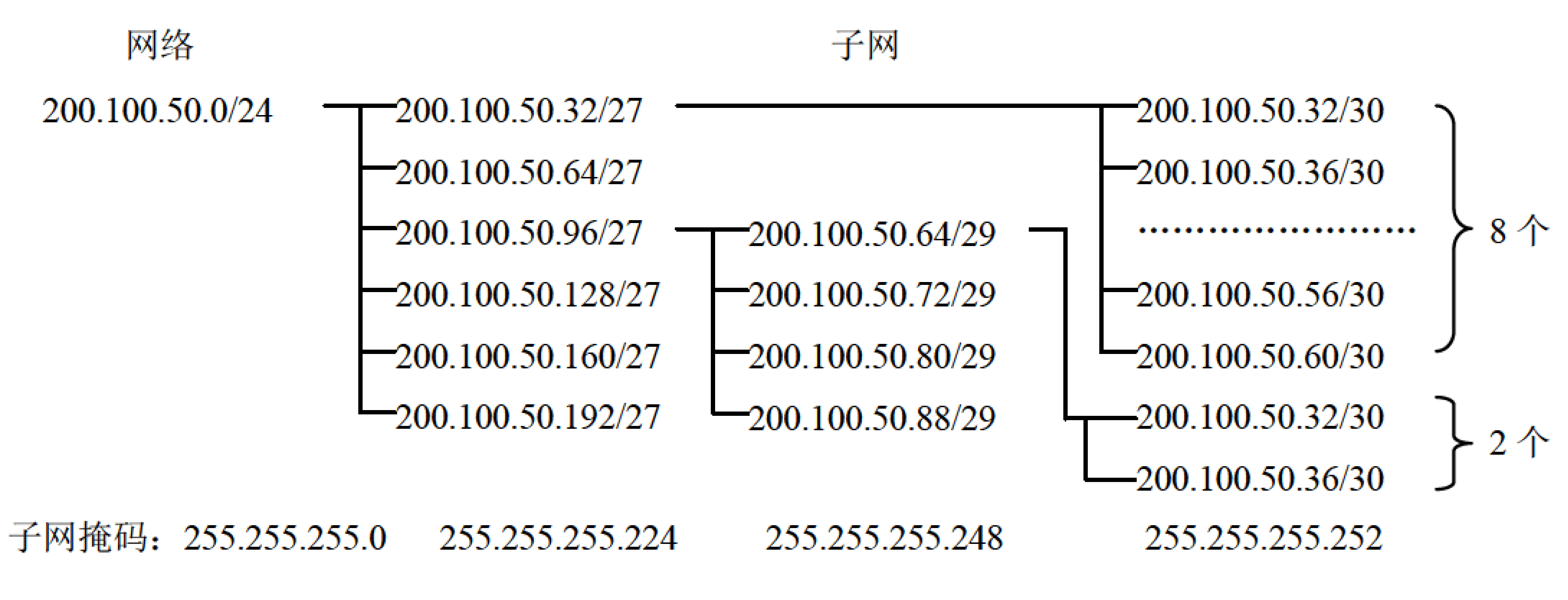



图 2-64 问题 1 解答

**【问题 2】**见问题 1

**【问题 3】**见问题 1

5.

**【问题 1】**存放在/etc/mail/local-host-names 文件中

**【问题 2】**210.45.45.0/24 这个 C 类网络中

**【问题 3】**xyz.com.tw　DENY

**【问题 4】**将发给 zhang 这个用户，邮件服务器地址是 zhang@abc.com.cn

**【问题 5】**创建传送控制配置文件 Access 相应的数据库文件

6.

**【问题 1】**172.16.0.1～172.168.255.253、255.255.0.0

**【问题 2】**8080

**【问题 3】**/cache1、4000MB、24、33

**【问题 4】**202.102.192.68

**【问题 5】**禁止客户访问域 foo.com.tw 内的所有主机

7.

**【问题 1】**请求 IP 租约、提供 IP 租约、选择 IP 租约和确认 IP 租约

**【问题 2】**广播方式

**【问题 3】**DHCP 服务器应具有静态 IP 和子网掩码，有一组可供分配的 IP 地址。

**【问题 4】**ipconfig/all、ipconfig/renew、ipconfig/release

8.

**【问题 1】**/etc/httpd

**【问题 2】**用文档/missing.html 来回应客户浏览器

**【问题 3】**建立一个域名为 markert.abc.com.cn 的虚拟 Web 服务器(虚拟主机)，并指定相应的参数。

**【问题 4】**访问该服务器中用户 zhang 的主目录下 public_html 子目录的索引文件 index.html，若该文件不存在就会出错。

**【问题 5】**#/etc/init.d/httpd stop

# 第 3 章　网络安全设置

**大纲要求：**

- 防火墙技术和入侵检测系统，包括防火墙的配置策略、入侵处理策略、漏洞处理策略。
- 病毒及病毒防范。
- 加密、认证、数字签名等安全技术，包括 DES 和 RSA 的基本概念、认证、数字证书、安全电子邮件、HTTPS。

## 3.1　网络病毒防护策略和入侵处理策略

### 3.1.1　考点辅导

#### 3.1.1.1　网络病毒简介

1. 网络病毒定义

网络病毒是指在网络上传播的计算机病毒，可能会为网络带来灾难性的后果，被称为“第二代病毒”。

2. 网络病毒的特点

网络病毒的特点及危害性主要表现在破坏性强、传播性强、具有潜伏性和可激发性、针对性强、扩散面广、传播速度快及难以彻底清除等。

3. 黑客的攻击手段

涉及网络安全的问题很多，但最主要的问题还是人为攻击，黑客就是最具有代表性的一类群体。黑客的出现可以说是当今信息社会，尤其是在因特网互联全球的过程中，网络用户有目共睹、不容忽视的一个独特现象。

常见的黑客攻击手段有以下几个。

1) 口令入侵

口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。使用这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。通常，黑客会利用一些系统使用习惯性账号的特点，采用字典穷举法(或称暴力法)来破解用户的密码。

2) 放置特洛伊木马程序

从严格的定义来讲，凡是非法驻留在目标计算机中，在目标计算机系统启动的时候自动运行，并在目标计算机上执行一些事先约定的操作(如窃取口令等)的程序都可以称为特洛

伊木马程序，即 Trojans。

特洛伊木马程序一般分为服务器端(Server)和客户端(Client)。服务器端是攻击者传到目标机器上的部分，用来在目标机上监听以等待客户端连接过来；客户端是用来控制目标机器的部分，放在攻击者的机器上。

3)　DoS 攻击

造成拒绝服务(Denial of Service，DoS)的攻击行为被称为 DoS 攻击，其目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击是指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终导致计算机无法再处理合法的用户请求。

分布式拒绝服务(Distributed Denial of Service，DDoS)攻击是指借助客户机/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。

4)　端口扫描

端口扫描就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。常用的扫描方式有 TCP connectU 扫描、TCP SYN 扫描、TCP FIN 扫描、IP 段扫描和 FTP 返回攻击等。

5)　网络监听

网络监听在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，因而一直备受网络管理员的青睐。然而，网络监听也给以太网的安全带来了极大的隐患，许多的网络入侵往往都伴随着以太网内的网络监听行为，从而造成口令失窃、敏感数据被截获等连锁性安全事件。

Sniffer 是一款著名的监听工具，它可以监听到网上传输的所有信息。Sniffer 可以是硬件也可以是软件，主要用来接收在网络上传输的信息。

6)　欺骗攻击

欺骗攻击是攻击者创造一个易于误解的上下文环境，以诱使受攻击者进入并且做出缺乏安全考虑的决策。

常见的欺骗攻击如下。

(1)　Web 欺骗。Web 欺骗允许攻击者创造整个 WWW 世界的影像副本。影像 Web 的入口进入到攻击者的 Web 服务器，经过攻击者机器的过滤作用，允许攻击者监控受攻击者的任何活动，包括账户和口令。攻击者观察和控制着受攻击者在 Web 上所做的每一件事。

(2)　ARP 欺骗。通常源主机在发送一个 IP 包之前，它要到该转换表中寻找和 IP 包对应的 MAC 地址。此时若入侵者强制目的主机 Down 掉(如发洪水包)，同时把自己主机的 IP 地址改为合法目的主机的 IP 地址，然后它发一个 ping ( icmp 0 )给源主机，要求更新主机的 ARP 转换表，主机找到该 IP，然后在 ARP 表中加入新的 IP->MAC 对应关系。这样合法的目的主机就失效了，入侵主机的 MAC 地址变成了合法的 MAC 地址。

(3)　IP 欺骗。IP 欺骗由若干步骤组成。首先，目标主机已经选定；其次，信任模式已被发现，并找到了一个被目标主机信任的主机。黑客为了进行 IP 欺骗，需要进行以下工作：

使得被信任的主机丧失工作能力，同时采样目标主机发出的 TCP 序列号，从而猜测出它的数据序列号。然后伪装成被信任的主机，同时建立起与目标主机基于地址验证的应用连接。如果成功，黑客可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

7) 电子邮件攻击

电子邮件攻击主要表现为向目标信箱发送电子邮件炸弹。电子邮件炸弹实质上就是发送地址不详且容量庞大的垃圾邮件。因为相对于其他的攻击手段来说，这种攻击方法具有简单、见效快等优点。

电子邮件欺骗也是黑客常用的手段。黑客们常会佯称自己是系统管理员(邮件地址和系统管理员完全相同)，给用户发送邮件，要求用户修改口令(口令有可能为指定的字符串)或在貌似正常的附件中加载病毒或某些特洛伊木马程序。

### 3.1.1.2 基于网络的防病毒系统

1. 网络防病毒需求

目前，Internet 已经成为病毒传播的最大途径，电子邮件和网络信息的传递为病毒传播打开了高速的通道。各行各业网络化的发展也使病毒的传播速度大大提高，感染的范围也越来越广。可以说，网络化带来了病毒的高效率，而病毒的高效率也对防病毒产品提出了新的要求。

2. 网络病毒传播方式

一般来说，计算机网络的基本构成为网络服务器和网络节点站(包括有盘工作站、无盘工作站和远程工作站)。计算机病毒一般首先通过有盘工作站传播到软盘和硬盘，然后进入网络，进一步在网上传播。具体来说，其传播方式有以下几种。

(1) 病毒直接从有盘工作站复制到服务器中。

(2) 病毒先传染工作站，在工作站内存中驻留，等运行网络盘内程序时再传染给服务器。

(3) 病毒先传染工作站，在工作站内存中驻留，在运行时直接通过映像路径传染到服务器。

(4) 如果远程工作站被病毒侵入，病毒也可以通过通信过程中的数据交换进入网络服务器中。

3. 网络病毒防护策略

基于网络系统的病毒防护体系主要包括以下几个方面的策略。

1) 一定要实现全方位、多层次防毒

一定要部署多层次病毒防线，如网关防毒，群件服务器、应用服务器防毒和客户端防毒，保证斩断病毒可以传播、寄生的每一个节点，从而实现病毒的全面防范。

2) 网关防毒是整体防毒的首要防线

将网关防毒作为最重要的一道防线来部署，全面消除外来病毒的威胁，使得病毒不再从网络传播进来，以免对内部网资源和系统资源造成消耗。同时，网关防毒这道防线还必须具备内容过滤功能，以全面防范垃圾邮件的侵扰以及内部机密数据的外泄。


3)　缺乏管理的防毒系统是无效的防毒系统

为保证防毒系统有效、及时地拦截病毒，必须确保整个防毒产品可以从管理系统中及时得到更新，整个系统中任何一个节点都可以被管理人员随时管理。

4)　技术支持服务是整体防毒系统中极为重要的一环

病毒破坏系统的方法五花八门，病毒传播和感染的手段多种多样，新的病毒对防病毒软件自身破坏情况不断增多，这些都造成防病毒软件在具体实施和应用中会遇到各种各样的问题。因此，防病毒厂商能否及时、全面地提供解决方案及技术支持服务是能否对网络病毒进行有效防范极为重要的一环，另外要求厂商能有足够的本地化技术人员作为依托。

4. 网络防毒系统的组织形式

1)　系统中心统一管理

为了提高杀毒的效率和稳定性，可采用多级管理体系，由系统中心统一管理。中心可以控制网络内的所有机器统一杀毒，在同一时间查杀所有病毒，从而解决网络环境下机器的重复感染问题。

2)　远程安装升级

网络病毒防护系统提供远程安装和用户通过 Web 页面下载客户端自行安装两种方式，客户端能自动从系统中心升级。

3)　一般客户端的防毒

系统中心可以控制客户端的杀毒软件，由系统中心统一组织杀毒；客户端也可自行查杀，并将结果报送系统中心。服务器端的查杀操作应与客户端一致，区别在于软件是为服务器专门设计的杀毒软件。

4)　防病毒过滤网关

防病毒过滤网关实际上就是企业级病毒防火墙，通常通过部署在用户内部网与外部网的接入点，实现邮件病毒过滤及 Internet 病毒过滤。它可以简单、高效地对用户网络可能遇到的来自 Internet 的病毒威胁提供强有力的深层病毒防护。

5)　硬件防病毒网关

与客户端、服务器软件类防毒产品相比，硬件防毒网关类产品具有以下特色。

(1) 高效稳定。硬件防毒网关类产品由于采用独立的硬件平台，大大提高了系统的稳定性和查杀病毒的效率。

(2) 操作简单、管理方便。硬件防毒网关类产品一般采用 B/S 管理构架，友好的图形管理界面可供用户方便地对设备进行简单、易行的配置。

(3) 接入方式简单易行。

(4) 免维护。远程自动更新代码和系统升级，无须管理员日常维护。

(5) 容错与集群。系统通过集群模块，在容错的同时线性地增加处理能力，从而满足高带宽的网关杀毒需要。

### 3.1.1.3　入侵检测系统部署

1. 部署实例

对于入侵检测系统来说，其类型不同、应用环境不同，部署方案也就会有所差别。对于基于主机的入侵检测系统来说，一般用于保护关键主机或服务器，因此只要将它部署到

这些关键主机或服务器中即可。但是对于基于网络的入侵检测系统来说，因各种网络环境千差万别，根据网络环境的不同其部署方案也会有所不同。

1) 共享部署

在共享介质的环境下，传感器能够监听到整个冲突域内的流量，所以只需要把传感器的监听端口接到 Hub 上即可，如图 3-1 所示。

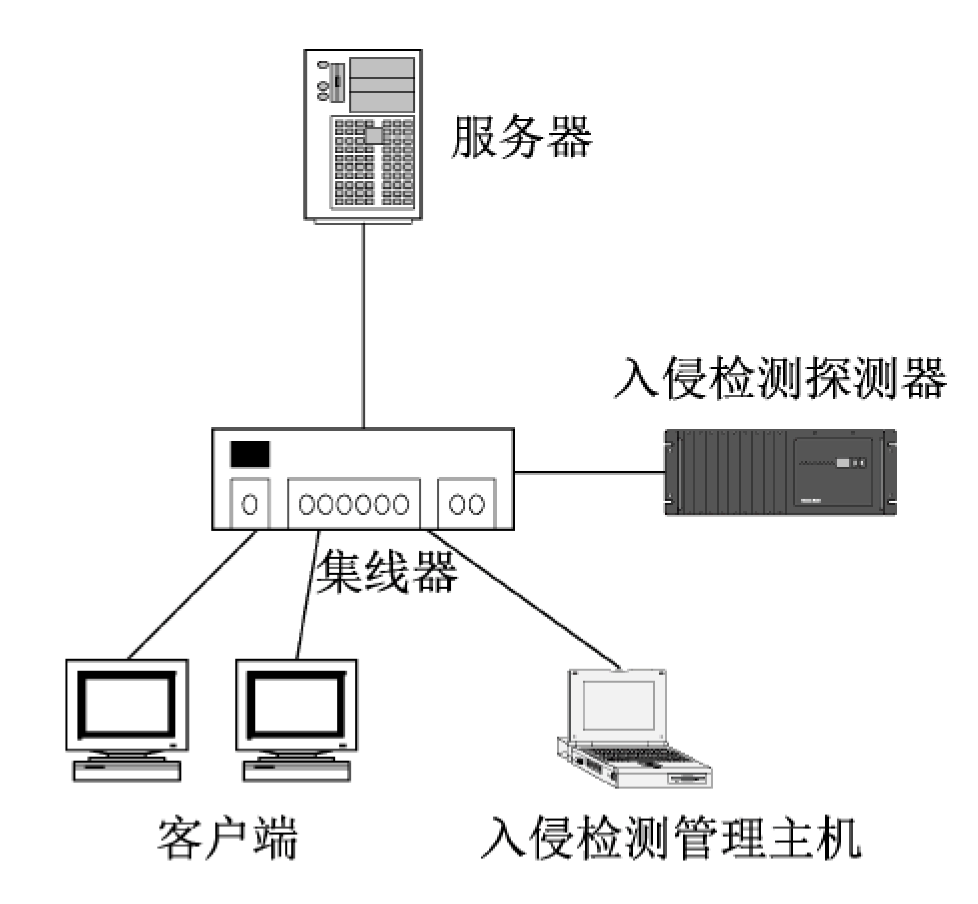



图 3-1 共享介质环境下入侵检测的部署

2) 交换环境

在交换环境下，每个交换机的端口都是一个独立的冲突域，因此传感器不能直接监听到交换机其他端口的流量。通常可以采用以下几种方法解决此问题。

(1) 在交换机和路由器之间接入一个集线器，从而把一个交换环境转换为共享环境。这样做的优点是简单易行、成本低廉。如果客户对网络的传输速度和可靠性要求不高，建议采用这种方法，如图 3-2 所示。

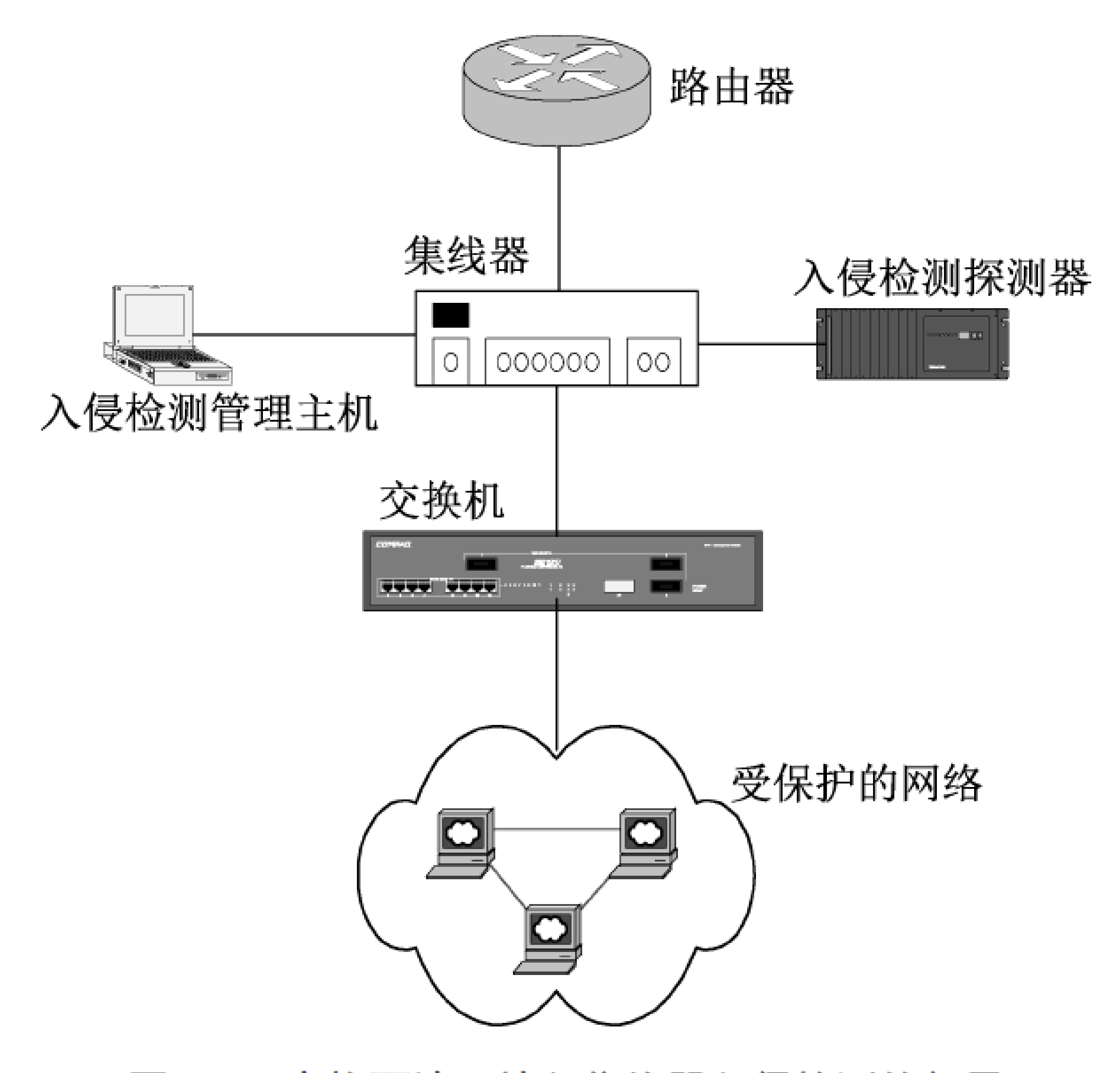



图 3-2 交换环境下接入集线器入侵检测的部署

(2) 如果交换机支持端口镜像功能，建议采用以下方法：在不改变原有网络拓扑结构的基础上完成传感器的部署。其优点是配置简单、灵活，使用方便，不需中断网络。这是比较常用的一种方式，如图 3-3 所示。

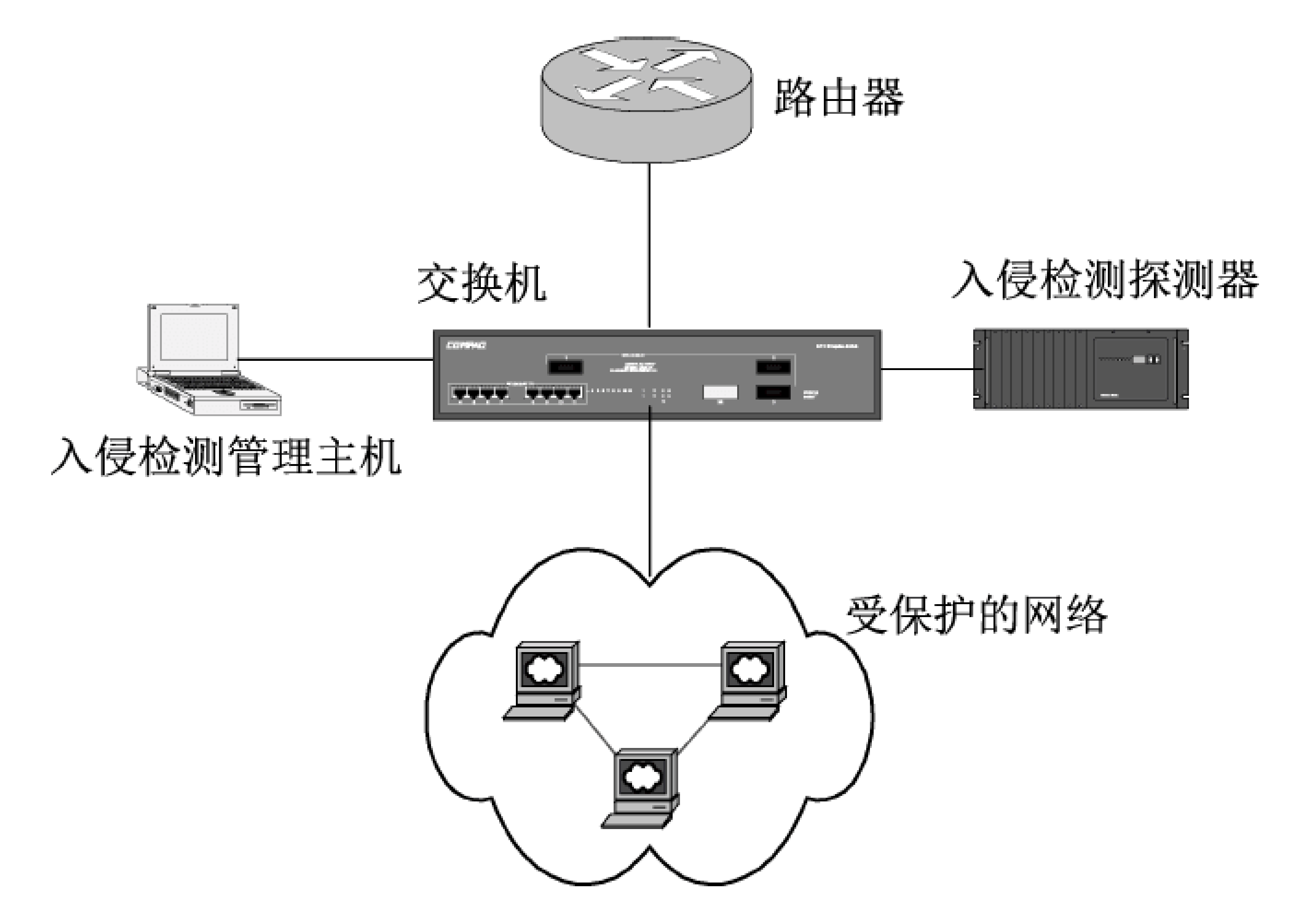



图 3-3　交换环境下入侵检测的部署

(3) 如果交换机不支持端口镜像功能，或者出于性能的考虑不便启用该功能，可以采用 TAP(分支器)。它的优点是能够支持全双工 100Mb/s 或者全双工 1000Mb/s 的网络流量。

2. 典型应用

本实例假设所采用的交换机支持端口镜像功能。

1) 小规模网络环境

此种区域网连接方法较为简单，内部网络中各机构的主机使用共享式集线器连接到交换机上，或主机直接连接到交换机上，交换机不设 VLAN，交换机再通过路由器接入 Internet。在这种情况下，将 IDS 监测主机接到交换机的广播口(监听口)即可监听到内部网络间的所有通信及内部网络到 Internet 的所有通信，如图 3-4 所示。

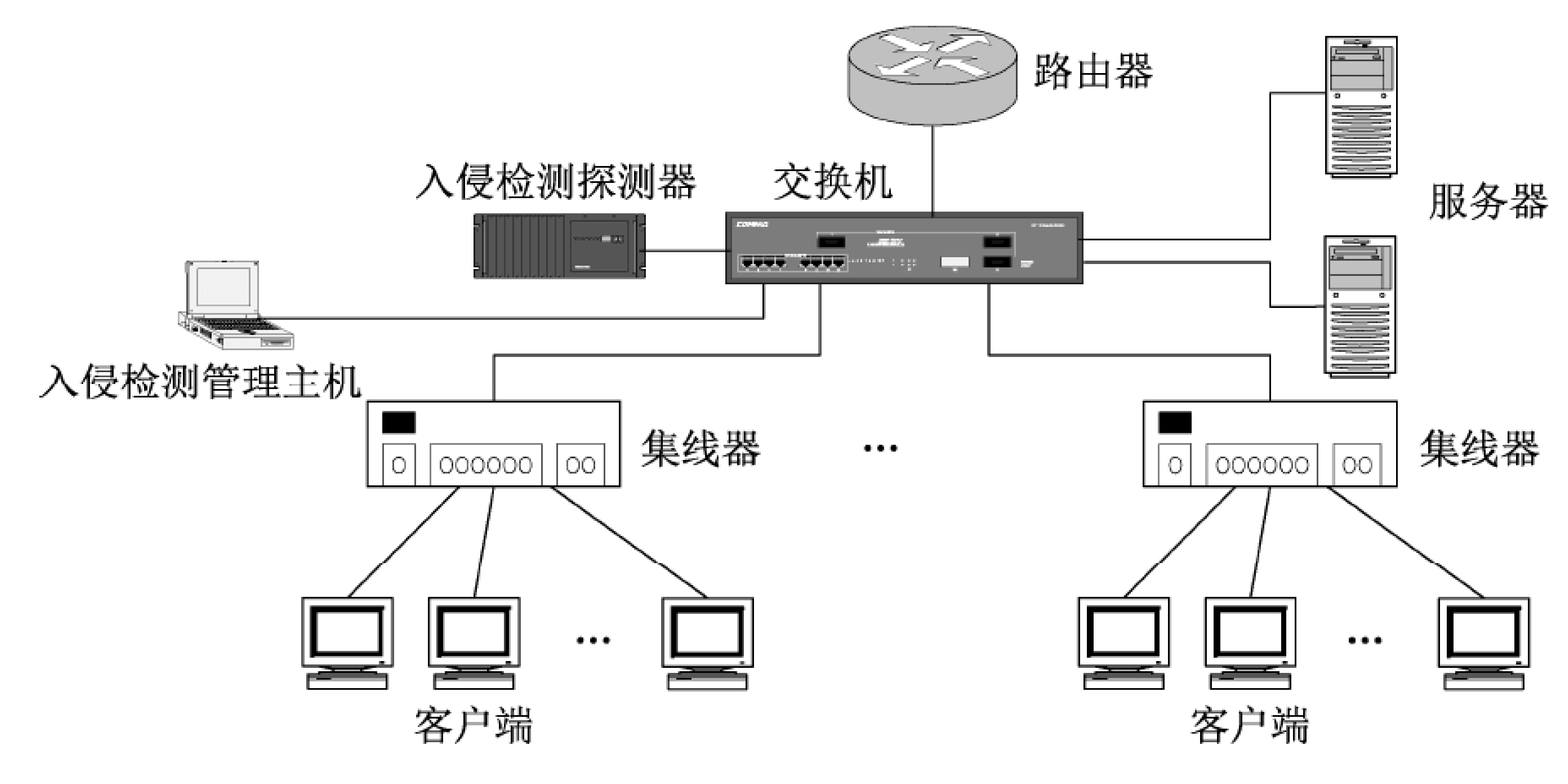



图 3-4　小规模网络环境应用

2) 分布式监测应用示例

网络结构相对较复杂，内部网络中各机构间使用交换机连接到主交换机上，通过主交换机连接路由器接入 Internet。此时在主交换机的广播口(监听口)上无法监听到从交换机上的机器间的通信，为了全面监控网络，捕捉内部网间的恶意攻击与入侵行为，就需要为每个重要的网段部署一个入侵检测探测器，并分别将检测到的事件发送到集中管理控制台，如图 3-5 所示。

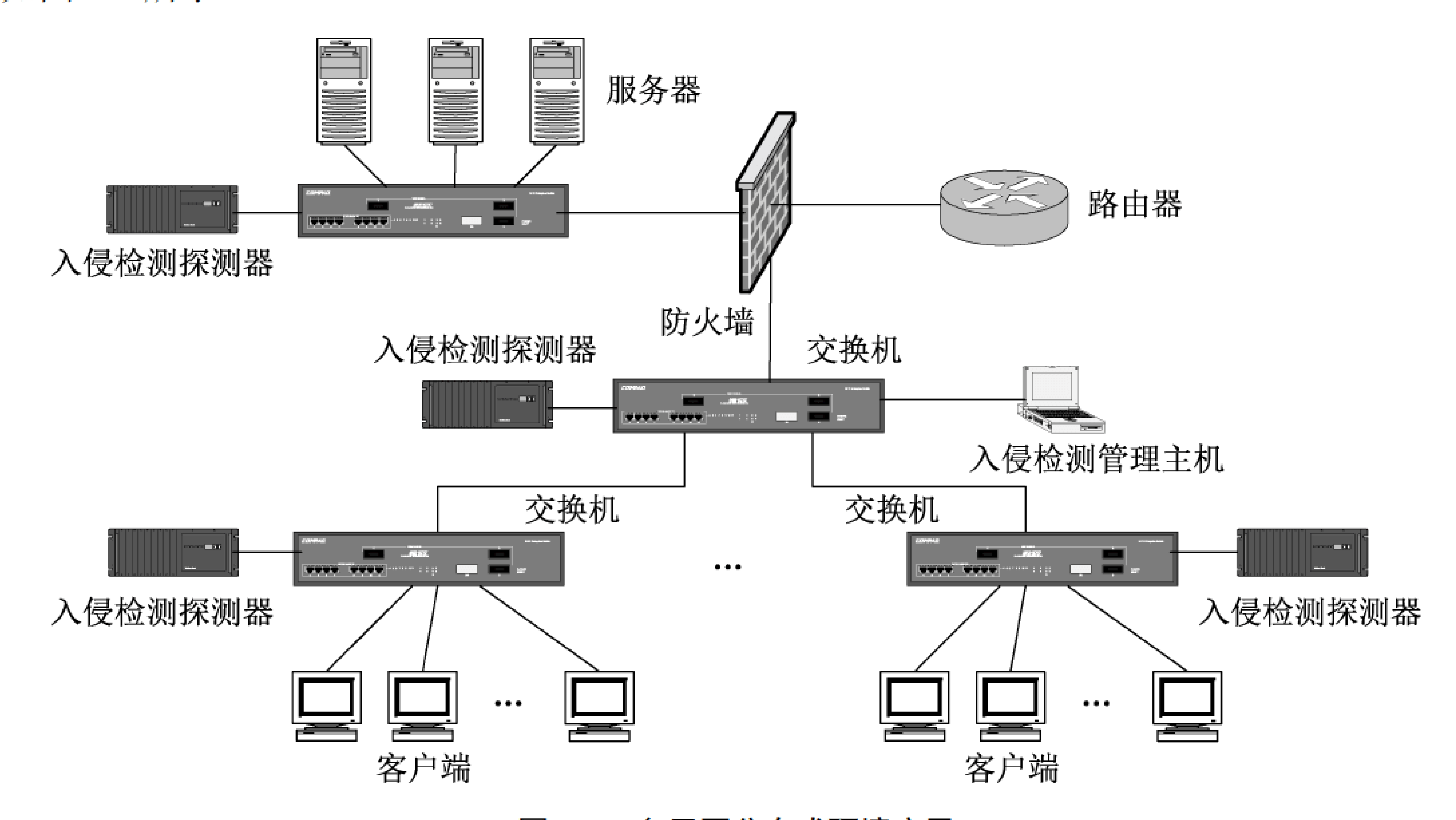



图 3-5 多子网分布式环境应用

## 3.1.2 典型例题分析

**例 1** 阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。(2006 年 11 月下午试题四)

**【说明】**

特洛伊木马是一种基于客户机/服务器模式的远程控制程序，黑客可以利用木马程序入侵用户的计算机系统。木马的工作模式如图 3-6 所示。

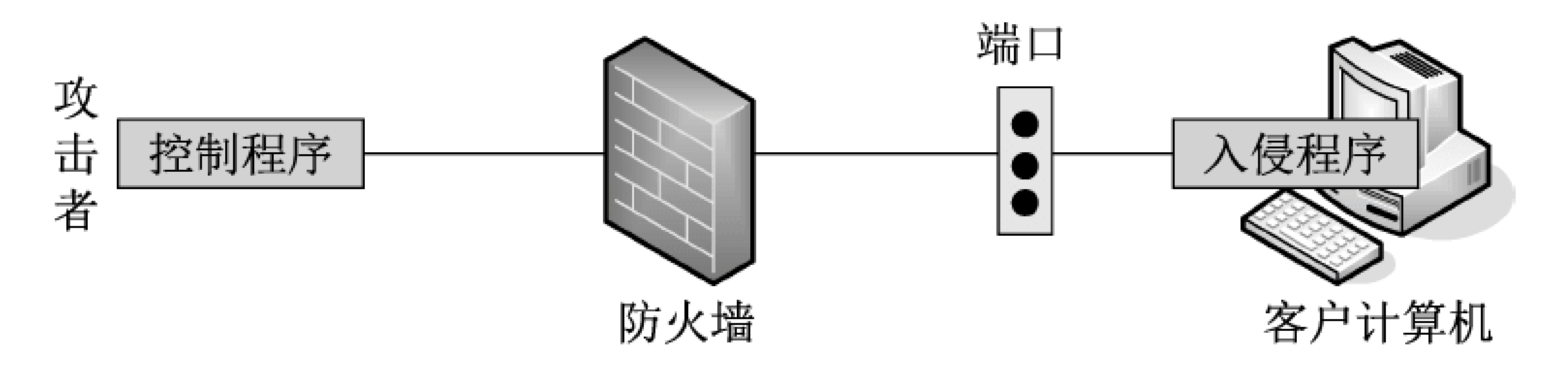



图 3-6 木马工作原理示意

**【问题 1】**(2 分)

对于传统的木马程序，侵入被攻击主机的入侵程序属于__(1)__。攻击者一旦获取入侵程序的__(2)__，便与它连接起来。

(1)　A. 客户程序　　B. 服务程序　　C. 代理程序　　D. 系统程序
(2)　A. 用户名和口令　　B. 密钥　　C. 访问权限　　D. 地址和端口号

**【问题 2】**(2 分)

以下__(3)__和__(4)__属于计算机感染特洛伊木马后的典型现象。

A. 程序堆栈溢出　　B. 有未知程序试图建立网络连接
C. 邮箱被莫名邮件填满　　D. 系统中有可疑的进程在运行

**【问题 3】**(2 分)

为了检测系统是否有木马侵入，可以使用 Windows 操作系统的__(5)__命令查看当前的活动连接端口。

A. ipport　　B. netstat-an　　C. tracert-an　　D. ipconfig

**【问题 4】**(4 分)

入侵程序可以通过修改 Windows 操作系统的__(6)__、__(7)__文件或修改系统中的相关注册表项实现系统启动时自动加载。通过运行 Windows 操作系统中的__(8)__(填空)命令，可以启动注册表编辑器来对注册表进行维护。

A. system.ini　　B. shell.ini　　C. win.ini　　D. autoexec.ini

**【问题 5】**(2 分)

安装了防火墙软件的主机可以利用防火墙的__(9)__功能有效地防止外部非法连接来拦截木马。

A. 身份认证　　B. 地址转换　　C. 日志记录　　D. 包过滤

**【问题 6】**(3 分)

以下措施中能有效防止木马入侵的有__(10)__和__(11)__。

A. 不随意下载来历不明的软件
B. 仅开放非系统端口
C. 实行加密数据传输
D. 运行实时网络连接监控系统

**分析：**

**【问题 1】**

特洛伊木马是一种基于客户端/服务器模式的远程控制程序，它可以让用户的机器运行服务器端的程序，该程序会在用户的计算机上打开监听的端口。这样就给黑客入侵用户计算机打开了一扇进出的门，黑客就可以利用木马程序的客户端入侵用户的计算机系统。因此，对于传统的木马程序，侵入被攻击主机的入侵程序属于服务器端程序，而攻击者掌握的是客户端程序，攻击者要想与入侵程序连接起来，需要得到入侵程序的地址和端口号。

**【问题 2】**

用户的计算机感染特洛伊木马后会受到木马程序的控制，典型的现象有以下几种。

(1)　死机、重启，长时间读写硬盘、搜索软盘。
(2)　运行速度越来越慢，资源占用多。
(3)　任务表中有可疑的文件在运行。

**【问题 3】**

当前最为常见的木马程序通常是基于 TCP/UDP 协议进行 Client 端与 Server 端之间通信

的，因此，可以通过查看在本机上开放的端口，来判断是否有可疑的程序打开了某个可疑的端口。查看端口的方法有以下几种。

- 使用 Windows 本身自带的 netstat 命令。例如：

```
C:\>netstat -an
```

- 使用 Windows 2000 下的命令行工具 fport，例如：

```
E:\software>Fport.exe
```

- 使用图形化界面工具 Active Ports。该工具可以监视到计算机所有打开的 TCP/IP/UDP 端口，还可以显示所有端口对应的程序所在的路径，本地 IP 和远端 IP 是否正在活动。这个工具适用于 Windows NT/2000/XP 平台。

**【问题 4】**

基于 Windows 的木马程序一般采用启动时自动加载应用程序的方法。其主要包括两种方法：一是修改 win.ini 和 system.ini 系统配置文件；二是修改注册表项。

**【问题 5】**

随着防火墙技术的提高和发展，基于 IP 包过滤规则来拦截木马程序可以有效地防止外部连接，因此黑客在无法取得连接的情况下也无所作为。

**【问题 6】**

随着网路的广泛应用、硬件和软件的高速发展，网络安全显得日益重要。对于网络中比较流行的木马程序，传播速度比较快，影响比较严重，因此对于木马程序的防范就更不能疏忽。用户在检测清除木马程序的同时，还要注意对木马程序的预防，做到防患于未然。

具体应做到以下几点。

(1) 不要随意打开来历不明的邮件。

(2) 不要随意下载来历不明的软件。

(3) 及时修补漏洞和关闭可疑的端口。

(4) 尽量少用共享文件夹。

(5) 运行实时监控程序。

(6) 经常升级系统和更新病毒库。

**答案：**

**【问题 1】**

(1) B

(2) D

**【问题 2】**

(3) B

(4) D

说明：(3)、(4)可以互换。

**【问题 3】**

(5) B

**【问题 4】**

(6) A

(7) C

说明：(6)、(7)可以互换。

(8) regedit

**【问题 5】**

(9) D

**【问题 6】**

(10) A

(11) D

说明：(10)、(11)可以互换。

## 3.1.3　同步练习

1．简述网络病毒防护策略。

2．简述网络防病毒的组织形式。

3．简述硬件防病毒网关的特色(与客户端、服务器软件类防毒产品相比)。

4．简述网络病毒的特点。

5．为了防范 Internet 的病毒对企业内部网的威胁，企业内部可购置什么防护系统？此系统应部署在什么地方？

## 3.1.4　同步练习参考答案

1、2、3、4 题答案见本节考点辅导。

5．为了防范因特网的病毒对企业内部网的威胁，企业内部可购置防病毒过滤网关防护系统。此系统部署在用户内部网与外部网的接入点处。

# 3.2　防火墙的配置策略和漏洞处理策略

## 3.2.1　考点辅导

### 3.2.1.1　防火墙概述

1．什么是防火墙

防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合。它对两个或多个网络之间的通信进行控制，通过强制实施统一的安全策略，来防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。

2．防火墙的相关概念

防火墙的相关概念有非信任网络(公共网络)、信任网络(内部网络)、DMZ(非军事化区)、

可信主机、非可信主机、公网 IP 地址、保留 IP 地址、包过滤、地址转换。

(1) 非信任网络(公共网络)。处于防火墙之外的公共开放网络，一般指 Internet。

(2) 信任网络(内部网络)。位于防火墙之内的可信网络，是防火墙要保护的目标。

(3) DMZ(非军事化区)。也称周边网络，可以位于防火墙之外，也可以位于防火墙之内。安全敏感度和保护强度较低。非军事化区一般用来放置提供公共网络服务的设备。这些设备由于必须被公共网络访问，所以无法提供与内部网主机相等的安全性。

(4) 可信主机。位于内部网的主机，且具有可信任的安全特性。

(5) 非可信主机。不具有可信特性的主机。

(6) 公网 IP 地址。由 Internet 信息中心统一管理分配的 IP 地址，可在 Internet 上使用。

(7) 保留 IP 地址。专门保留用于内部网的 IP 地址。可以由网络管理员任意指派，在 Internet 上不可识别和不可路由，如 192.168.0.0 和 10.0.0.0 等地址网段。

(8) 包过滤。防火墙对每个数据包进行允许或拒绝的决定。具体地说，就是根据数据包的头部按照规则进行判断，决定继续转发还是丢弃。

(9) 地址转换。防火墙将内部网主机不可路由的保留地址转换成公共网络可识别的公共地址，可以达到节省 IP 和隐藏内部网络拓扑结构信息等目的。

### 3. 防火墙的特性

1) 防火墙的功能及优点

(1) 对进出的数据包进行过滤，过滤掉不安全的服务和非法用户。

(2) 监视 Internet 安全，对网络攻击行为进行检测和报警。

(3) 记录通过防火墙的信息内容和活动。

(4) 控制对特殊站点的访问，封堵某些禁止的访问行为。

(5) 防火墙能强化安全策略，执行系统规定的规则，仅允许符合规则的信息通过。

(6) 防火墙能有效地记录 Internet 上的活动。因为所有进出的信息都需要经过防火墙，所以防火墙可以记录信任网络和非信任网络之间发生的各种事件。

(7) 防火墙是一个安全策略的边防站。因为所有进出内部网的信息都必须通过防火墙，所以防火墙便成为一个安全检查站，能够把可疑的连接或者访问拒之门外。

2) 防火墙的缺点

(1) 防火墙不能防范不经过防火墙的攻击。未经过防火墙的数据，防火墙无法检查，如拨号上网。

(2) 防火墙不能解决来自内部网络的攻击和安全问题。对于防火墙内部各主机间的攻击行为，防火墙就爱莫能助。

(3) 防火墙不能防止最新的未设置策略或错误配置引起的安全威胁。因为防火墙的各种策略是在某攻击方式经过专家分析后给出其特征而设置的。

(4) 防火墙不能防止人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。

(5) 防火墙无法解决 TCP/IP 等协议的漏洞。防火墙本身就是基于 TCP/IP 等协议而实现的，因此就无法解决 TCP/IP 操作的漏洞，如 DoS 或 DDoS 攻击。

(6) 防火墙对服务器合法开放的端口的攻击大多无法阻止。

(7) 防火墙不能防止受病毒感染的文件传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒软件，也没有一种软件可以查杀所有的病毒。

(8) 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。

(9) 防火墙不能防止内部的泄密行为。对于内部的一个合法用户主动泄密，防火墙是无能为力的。

(10) 防火墙不能防止对本身安全漏洞的威胁。防火墙保护别人有时却无法保护自己，因为目前还没有厂商绝对保证防火墙不会存在安全漏洞。防火墙也有一个操作系统，也有着其硬件系统和软件，因此依然有着漏洞和 Bug，所以其本身也可能受到攻击和出现软件和硬件方面的故障。

4. 防火墙的基本分类

根据防火墙实现原理的不同，通常将防火墙分为包过滤防火墙、应用层网关防火墙和状态检测防火墙 3 类。

### 3.2.1.2　防火墙系统的安装与配置

下面主要以方正方御防火墙为例对防火墙的安装和配置进行说明。

1. 软、硬件安装

方御防火墙的软件部分主要由管理监控程序(FireControl)、串口配置程序(FCInit)和日志报警程序(LogService)组成。FireControl 是方御防火墙的管理程序，其作用是管理、监控、配置防火墙和设置入侵攻击报警策略，进行设备管理和日常监控；FCInit 的主要功能是初始化 FG 防火墙，它通过配置串口来完成初始化工作；LogService 的功能是获取日志、提供日志报警信息，在程序的安装过程中，能够自动装载数据和文件，并在系统程序组中生成方御防火墙的程序组。

方御防火墙的硬件名称为 FireGate(FG)。其硬件安装步骤如下。

(1) 用网线将外部网接口连接到 FG 的外部接口。

(2) 用网线将内部网接口连接到 FG 的内部接口。

(3) 用网线将控制主机连接到 FG 的控制接口。

(4) 用网线将开放区服务器接到 DMZ 区接口。

(5) 用电源线将 FG 接上电源，硬件安装完成。

其硬件安装结构如图 3-7 所示。

2. 基本配置

FireControl 安装在控制机上，控制机可以是与 FireControl 网口相连的任意台机器；在 FireControl 安装程序完毕后，即可在桌面上找到它的快捷方式。

管理员第一次启动 FireControl 管理程序时，应使用在 FCInit 中新建实施域时创建的默认账号 admin 进行登录。登录成功后，为安全起见，建议即刻修改 admin 账号的密码，以策略管理员身份登录 FireControl。策略管理员可自定义防火墙的各种参数，配置个性化的防火墙。防火墙的基本配置包括以下几个方面。

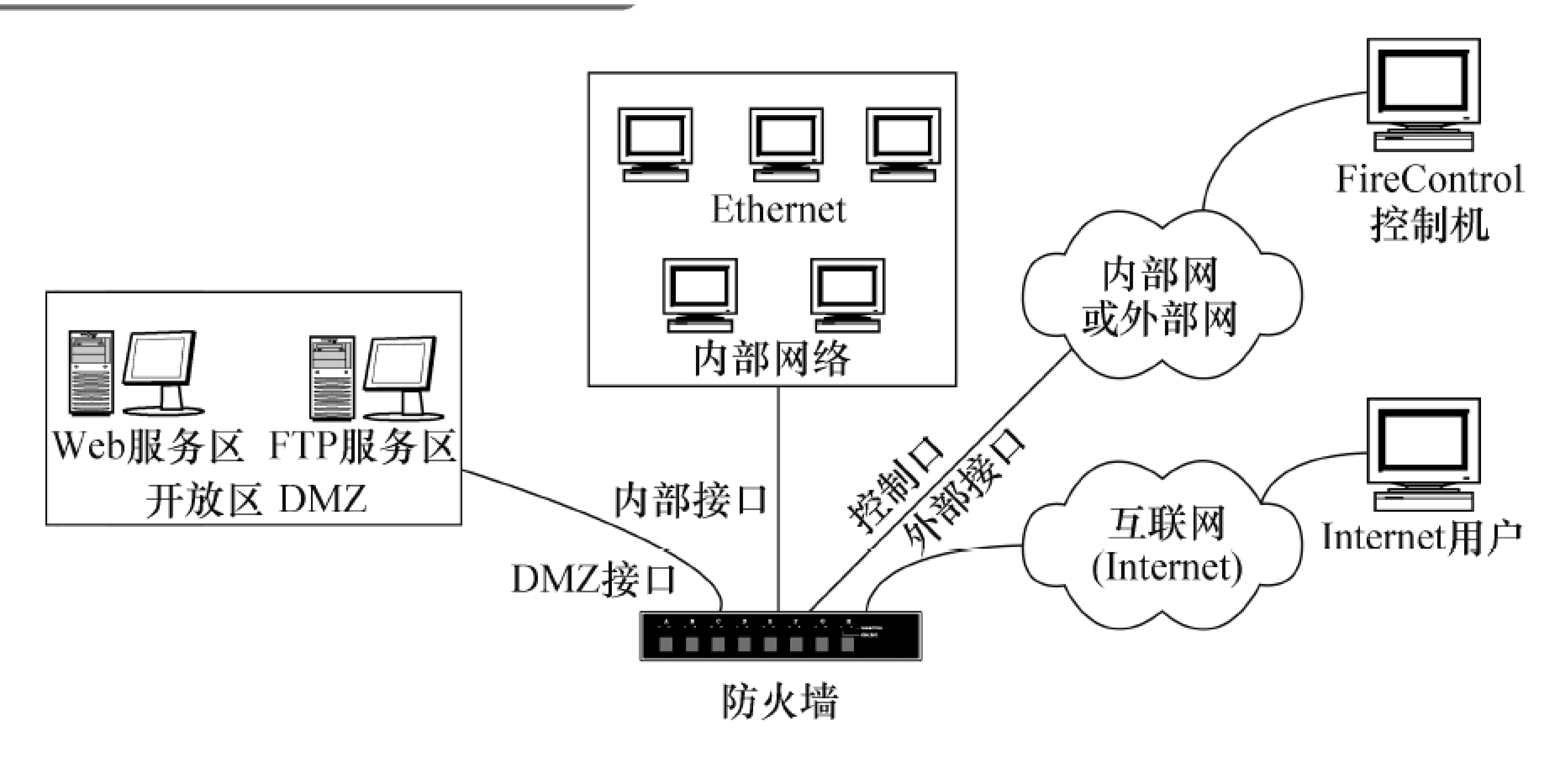


图 3-7　硬件安装结构

1)　别名

别名配置是指为相关网络地址和端口设置别名。别名的设计是为了方便策略管理员的使用。策略管理员可以使用好记的别名代替多个功能端口及子网，使配置不再烦琐。例如，使用别名 www 代替端口 80 或 8080，别名 office 代替 IP 地址为 105.118.0.0、子网掩码为 255.255.255.0 的网段地址，或者把几个离散的端口值和网段地址统一用一个别名进行管理。

别名是 FG 防火墙中重要的特性，大部分防火墙规则的配置都是通过别名来实现的，策略管理员在配置安全规则时需要先定义好相关的网络地址和端口的别名。

2)　设备配置

设备配置是防火墙自身的网络设置，包括对接口设备的配置和显示防火墙的基本信息。在 FG 初始化完成，以策略管理员身份登录后，首先需要进行设备配置，用户可以根据自己实际的网络需求在设备配置模块中通过对网络接口的设置实现多种工作模式。

防火墙可以有 3 种工作模式，即桥模式、路由模式和混杂模式。

(1)　桥模式。如果用户不想改变原有的网络拓扑结构和设置，可以将防火墙设置成桥模式。在桥模式下，网络间的访问是透明的，所有网口设备将构成一个网桥。

(2)　路由模式。这是防火墙的基本工作模式。在路由模式下，防火墙的各个网口设备的 IP 地址都位于不同的网段。

(3)　混杂模式。它指防火墙部分网口在路由模式下工作，部分网口在桥模式下工作。即某些子网之间以路由方式通信，而某些子网之间可以透明通信。

3)　SNMP 配置

FG 支持 SNMP(简单网络管理协议)。一方面，网络管理工具可以实时获取 FG 的状态，为其提供相关的系统状态、网络接口状态、IP 状态、ARP 表状态和 SNMP 服务状态等信息；另一方面，FG 为网络管理平台定期提供有关 FG 防火墙的信息，如入侵信息、管理信息和系统信息。

SNMP 的界面配置可分为以下 4 个部分。

(1)　防火墙位置标识：对系统本地位置信息进行配置。

(2)　共同体(Community)：用于简单的权限控制，默认为 public。

(3)　SNMP 管理服务器地址：网络管理服务器地址。

(4)　管理服务器 Trap 服务端口：网络管理服务器 Trap 接收端口，默认为 162。

4)　双机热备份技术

双机热备份是指一台 FG 为主机，正常情况下处于工作状态，另一台 FG 作为备用机，平时处于备用状态，并不工作，当工作状态的系统出现故障时，备用状态的防火墙在保证网络正常使用的情况下，可立即自动切换到工作状态，接替主机的角色，承担防火墙的工作。

方御防火墙系统在桥模式下能够在网络中智能地寻找其对等的备份机，并且使备份机自动进入等待状态，而一旦备份机发现主工作机失效，可及时地启动，防止网络中断事故的发生。要保护网络的安全，防火墙本身首先要安全。即使防火墙未被黑客攻击，也会由于元器件老化、异常死机等特殊原因发生故障。一旦发生故障，网络的安全就无法保证。对可靠性要求很高的用户，一定要选用有双机热备份技术的防火墙。FG 在路由模式下的双机热备份需要手工设置。

双机热备份连接如图 3-8 所示。防火墙的 COM 2 口需要用串口线连接；两台 FG 的内部、外部、DMZ 区以及控制接口需要分别通过交换机或集线器用网线连接。硬件连接完成后，需要在 FG 控制端进行设置。只有策略管理员可以设置双机热备功能。双机热备份系统只在桥模式和路由模式下工作，不支持混杂模式及 VLAN。

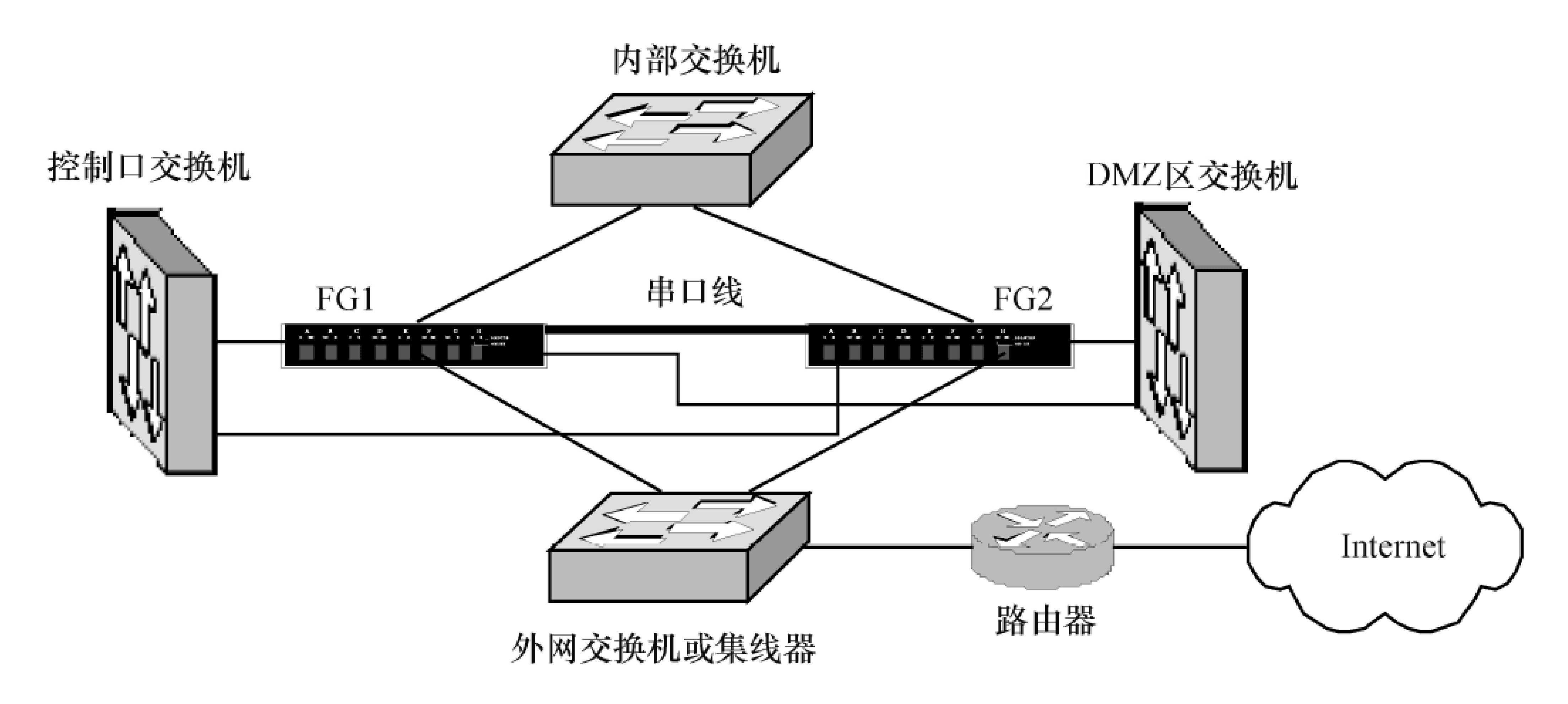



图 3-8　双机热备份连接示意

3. 规则配置

FG 防火墙提供基于状态检测技术的包过滤，能够根据数据包的地址、协议和端口进行访问控制。FG 防火墙包过滤功能主要是通过制定过滤规则集，对数据包头源地址、目的地址和端口号、协议类型等标志进行检查，以判定是否允许通过。对于满足过滤规则的数据包，可以选择放过或者丢弃，不满足规则的包则被丢弃。包过滤规则采用按顺序匹配的方式，即首先匹配前面的规则，若匹配则不再向下执行，因此一定要注意规则设置的顺序问题。

防火墙的规则配置是面向网口设备的，每个网口上的规则是指：每个接口设备接收到的数据包要经过这些规则的过滤，此处的接口包括物理接口设备和 VLAN 设备。每条规则详细描述了源/目的地址、目的端口、协议、数据流向、状态检测和策略等信息。

策略包括 4 种，即禁止(DROP)、允许(ACCEPT)、用户认证(AUTH)和自动封禁(AUTO)。

- 允许：接收此包。
- 禁止：丢弃此包。
- 用户认证：对于分配了公网 IP 的内部用户，如果出于安全性考虑，管理员希望用户必须通过认证才能访问因特网，则需要在用户管理模块中选择一种认证方式(内置账号认证或第三方认证)，并且在防火墙模块的相应接口设备上(一般是内部网对应的网口)添加一条用户认证规则。
- 自动封禁：FG 启动入侵检测功能后，需要在防火墙模块相应接口设备(包括物理网口、VLAN 设备)上添加一条“自动封禁”规则，才能自动封禁入侵 IP。FG 的每个网口都可以自动封禁。一般情况下，要设置入侵检测功能的自动封禁，应选择物理网口进行监听。

#### 3.2.1.3 访问控制列表

1. 基本概念

(1) IP 包过滤技术。路由器在转发数据包时，先获取包头信息(包括 IP 层所承载的上层协议的协议号及数据包的源地址、目的地址、源端口号和目的端口号等)，然后与设定的规则进行比较，再根据比较的结果对数据包进行转发或者丢弃。

(2) IP 访问控制列表是实现包过滤的核心技术。访问控制列表就是一系列允许和拒绝条件的集合，通过访问控制列表可以过滤发进和发出的信息包的请求，实现对路由器和网络的安全控制。路由器逐个地检测包与访问列表的条件，在满足第一个匹配条件后就可以决定是接收还是拒收该包。

2. 访问控制列表的分类和配置

1) IP 访问控制列表的分类

(1) 标准访问控制列表。只对数据包中的源地址进行检查，而不考虑目的地址及端口号等过滤选项，表号为 1～99。

(2) 扩展访问控制列表。既检查包的源地址，也检查包的目的地址，还可以检查特殊的协议类型、端口以及其他参数，具有更大的自由度，表号为 100～199。

2) IP 访问控制列表的配置

(1) 配置步骤。

① 在全局配置模式下创建 ACL：

```
Router(config)#access-list access-list-number {permit | deny}
{test-conditions}
```

② 在接口配置模式下，使用 access-group 命令将 ACL 应用到某一接口上：

```
Router(config-if)#ip access-group access-list-number {in | out}
```

其中，in 和 out 参数可以控制接口中不同方向的数据包，如果不配置该参数，默认为 out。

(2) 创建访问控制列表。

- 通配符掩码。在创建访问控制列表，表示一定范围的 IP 地址时，不使用子网掩码而使用通配符掩码。通配符掩码可用 255.255.255.255 减去子网掩码求出。

- 在通配符掩码中，可以用 255.255.255.255 表示所有 IP 地址，也可以用 any 来取代。而 0.0.0.0 的通配符掩码则表示所有 32 位都要进行匹配，这样只表示一个 IP 地址，可以用 host 来表示。

① 创建标准访问控制列表：

```
Router(config)# access-list access-list-number {deny | permit}
                source  [source-wildcard ]
```

参数说明：access-list-number 是定义访问列表的编号，取值范围为 1～99；deny 或 permit 指定了允许还是拒绝数据包；source 是发送数据包的主机地址；source-wildcard 是发送数据包的主机的通配符掩码。

② 创建扩展访问控制列表：

```
Router(config)#access-list access-list-number {permit | deny}
    protocol {source [source-wildcard] |any }
    {destination [destination-wildcard] |any }
    [protocol-specific options] [established] [log]
```

参数说明如下。

- access-list-number：定义访问列表的编号，取值范围为 100～199。
- deny 或 permit：指定了允许还是拒绝数据包。
- protocol：协议，如 IP、TCP、UPD、ICMP、OSPF 等。
- source、destination、destination-wildcard：源地址和目标地址。
- source-wildcard：通配符掩码。
- protocol-specific options：指定协议选项，用 lt、eq、gt、neq(小于、等于、大于、不等于)加端口号来指定，如 eq 80。

#### 3.2.1.4　配置 Cisco PIX 防火墙

(1) 配置方法。基本上与路由器、交换机的相同，包括初始配置必须使用控制台端口(Console)方式，同时支持 Telnet、FTP 服务器等配置方式。

(2) 常用的配置命令有 nameif、interface、ip address、nat、global、route、conduit、telnet、write memory 等。

- 配置防火墙接口的名字，并指定安全级别(nameif)：

  ```
  Firewall(config)#nameif hardware_id interface security_level
  ```

  在默认配置中，以太网口 0 被命名为外部接口(Outside)，安全级别是 0；以太网口 1 被命名为内部接口(Inside)，安全级别是 100。安全级别取值范围为 1～99，数字越大安全级别越高。

- 配置网络接口参数(interface)：配置接口的参数，如双工、速率、启用或停用。

  ```
  Firewall(config)#interface hardware_id [hardware_speed] [shutdown]
  ```

- 配置内外网卡的 IP 地址(ip address)：ip address 用于手动配置一个接口上的 IP 地址，将一个逻辑地址添加到一个硬件 ID 上。

  ```
  Firewall(config)#ip address if_name ip_address [netmask]
  ```

- 指定外部地址范围(global)：把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。

```
Firewall(config)#global (if_name) nat_id ip_address-ip_address
    [netmask global_mask]
```

- 配置地址轮换(nat)：将内网的私有 IP 地址转换为外网的公有 IP 地址。nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

```
Firewall(config)#nat (if_name) nat_id local_ip [netmask]
```

- 设置指向内网和外网的静态路由(route)：route 告诉我们要在哪个特定的网口转发，并指定哪个网络地址。

```
Firewall(config)#route (if_name) 0 0 gateway_ip [metric]
```

- 设置某些控制选项(conduit)：用于允许数据包从较低安全级别流向较高安全级别。通常是外网对内网的访问。

```
Firewall(config)#conduit global_ip port[-port] protocol
    foreign_ip [netmask]
```

- 设置 telnet 选项(telnet)：在默认情况下，PIX 的以太网端口是不允许 Telnet 的，配置只能通过 Console 口，这一点与路由器有区别。可以通过 telnet 命令指定哪些计算机能够用 telnet 登录到防火墙。

```
Firewall(config)#telnet local_ip [netmask]
```

- 保存配置(write memory)：将运行的配置文件保存到 NVRAM 中。

```
Firewall(config)# write memory
```

- 测试命令如下：

```
Firewall(config)#ping                    (连通性测试)
Firewall(config)#show interface          (查看端口状态)
Firewall(config)#show static             (查看静态地址映射)
Firewall(config)#write terminal          (查看配置)
```

#### 3.2.1.5 其他设置

1. 安全套接层(SSL)

(1) SSL。提供了两台计算机之间的安全连接，对整个会话进行了加密，从而保证了安全传输。工作在应用层和传输层之间，但属于传输层协议。

(2) SSL 的体系结构如图 3-9 所示。

(3) SSL 的功能。具有 3 个基本功能，即验证身份、数据的机密性和报文的完整性。

(4) SSL 会话与 SSL 连接。

① 连接。是提供恰当类型服务的传输。对于 SSL，这样的连接是点对点的关系。连接是短暂的，每一个连接与一个会话相联系。

② 会话。SSL 的会话是客户与服务器之间的关联。会话通过握手协议来创建。

| | | | |
|---|---|---|---|
| HTTPS、FTPS、TELNETS、IMAPS 等 | | | 应用层 |
| SSL 握手协议 | SSL 修改密文协议 | SSL 告警协议 | SSL 层 |
| SSL 记录协议 | | | |
| TCP | | | 传输层 |
| IP | | | 网络层 |

图 3-9　SSL 协议与 TCP/IP 协议间的关系

(5) SSL 握手过程。由 SSL 握手来完成，其过程如下。

① SSL 客户机连接至 SSL 服务器，并要求服务器验证其自身的身份。

② 服务器通过发送它的数字证书证明其身份。这个交换还可以包括整个证书链，直到某个认证证书颁发机构(CA)认证为止。通过检查有效日期并确认证书包含可信任 CA 的数字签名来验证证书的有效性。

③ 服务器发出一个请求，对客户端的证书进行验证，但是由于缺乏公钥体系结构，当今的大多数服务器不进行客户端认证。

④ 协商用于加密的消息加密算法(如 IDEA、RC4、DES、3DES、RSA 等)和用于完整性检查的哈希函数(如 MD5、SHA 等)。通常由客户端提供它支持的所有算法列表，然后由服务器选择最强大的加密算法。

(6) 数据封装。SSL 记录协议从高层接收到数据后要经过分段、压缩和加密处理，最后由传输层发送出去，从而保证了数据的机密性和报文的完整性。其数据的封装过程如下。

① 分片。将上层交付的报文分成 $2^{14}$ 字节或更小的数据块。

② 可选地应用压缩。

③ 使用共享密钥计算报文鉴别代码(MAC)。

④ 使用同步算法加密报文。

⑤ 附加首部数据，包括内容类型、主要版本、次要版本及压缩长度。

⑥ 接收方接收到数据后，将其解密、验证、解压和重新装配，最后交回给高层用户。

### 2. 设置 IE 的 WWW 浏览环境

利用 IE 浏览因特网时，通常需要设置 WWW 的浏览环境。用户可以利用 IE 浏览器中的“工具”→“Internet 选项”菜单命令设置相应的浏览环境。

(1) 常规设置。可以设置主页、Internet 临时文件夹、历史记录及颜色、字体、语言和辅助工具等相关内容。

(2) 安全设置。用于设定或修改网络区域的安全级别。

(3) 隐私设置。是 IE 6.0 新加入的设置，主要包括隐私和弹出窗口设置。

(4) 内容设置。设置分组审查、证书和个人信息等。

(5) 连接设置。主要包括拨号和虚拟专用网设置以及局域网设置。

(6) 程序设置。用于指定 Windows 自动应用于 Internet 服务的程序。

(7) 高级设置。用于详细设定 IE 查看 Web 资源时的可选设置参数。

#### 3.2.1.6 漏洞处理策略

漏洞扫描系统是一种自动检测远程或本地主机安全性弱点的程序，是检测远程或本地系统安全脆弱性的一种安全技术。

1. 漏洞扫描工具

在网络安全策略的引导下，对网络可能存在的安全漏洞进行扫描，预先评估网络的安全性能，提供详细的网络安全隐患报告，找出网络的安全漏洞，给出网络漏洞修补建议是提高网络安全的重要措施，是保持网络安全的积极防御手段。网络漏洞扫描系统作为网络安全性的评估工具，一直受到网络安全产品提供商的重视，研发了具有不同特点的漏洞扫描工具。

漏洞扫描工具主要是静态对网络中的各种系统、设备和数据库进行漏洞扫描，找出整个网络系统中最容易受到攻击的地方，对网络进行有效的评估，最后提出建设性的解决方案。其工作原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。目标可以是工作站、服务器、交换机、数据库应用等各种对象。漏洞扫描工具可以分为 3 种，即基于服务器的扫描器、基于网络的扫描器和基于数据库的扫描器，可以分别对服务器、网络及数据库的安全漏洞进行扫描并提出安全分析报告。

2. 漏洞处理策略

漏洞形成的原因形形色色、不一而足，最常见的漏洞主要包含以下类型，即 CGI 脚本、POP3、FTP、SSH、HTTP、SMTP、IMAP、后门、RPC、DNS 漏洞等。根据不同的漏洞类型会有不同的漏洞处理策略。

### 3.2.2 典型例题分析

**例 1** 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2015 年 11 下午试题三)

**【说明】**

某公司网络拓扑结构如图 3-10 所示。公司采用光纤专线接入 Internet，要求公司内部 PC 机全部能够访问 Internet，同时还有两台服务器对外分别提供 Web 和 E-mail 服务。公司采 用 PLX 防火墙接入互联网。图 3-10 中两台交换机为普通二层交换机，路由器 R1 是与该公司互联的第一个 ISP 路由器。

**【问题 1】**

防火墙是一种位于内部网络与外部网络之间的网络安全设备。它有 3 种工作模式，分别为 (1) 、 (2) 和混合模式。

**【问题 2】**

请阅读以下防火墙的配置操作，按照题目要求补充完成(或解释)下列空白的配置命令或参数。

```
……
Pix#  (3)  .
Pix(config)#enable password cisco encry #  (4)
```

```
Pix(config)#interface eth0 auto
Pix(config)#interface eth1auto
Pix(config)#interface eth2auto
Pix(config)#nameif e0__(5)__security 100
Pix(config)#nameif e1__(6)__security 0
Pix(config)#nameif e2__(7)__security50
Pix(config)#ip add inside 192.168.1.1 255.255.255.0
Pix(config)#ip add outside 202.117.112.98 255.255.255.252
Pix(config)#ip add dmz 10.10.10.1 255.255.255.0
Pix(config)#nat (inside) 1 0 0   //__(8)__
Pix(config)#global(outside)1__(9)__
Pix(config)#static(dmz,outside)__(10)__202.117.112.98 80 10.10.10.2 80
netmask 255.255.255.255 0 0
Pix(config)#static(dmz,outside) tcp 202.117.112.98 443 10.10.10.2 443
netmask 255.255.255.255 0 0
Pix(config)#conduit permit tcp host 202.117.112.98 eq 80 any
Pix(config)#conduit permit tcp host 202.117.112.98 eq 443 any  //__(11)__
```

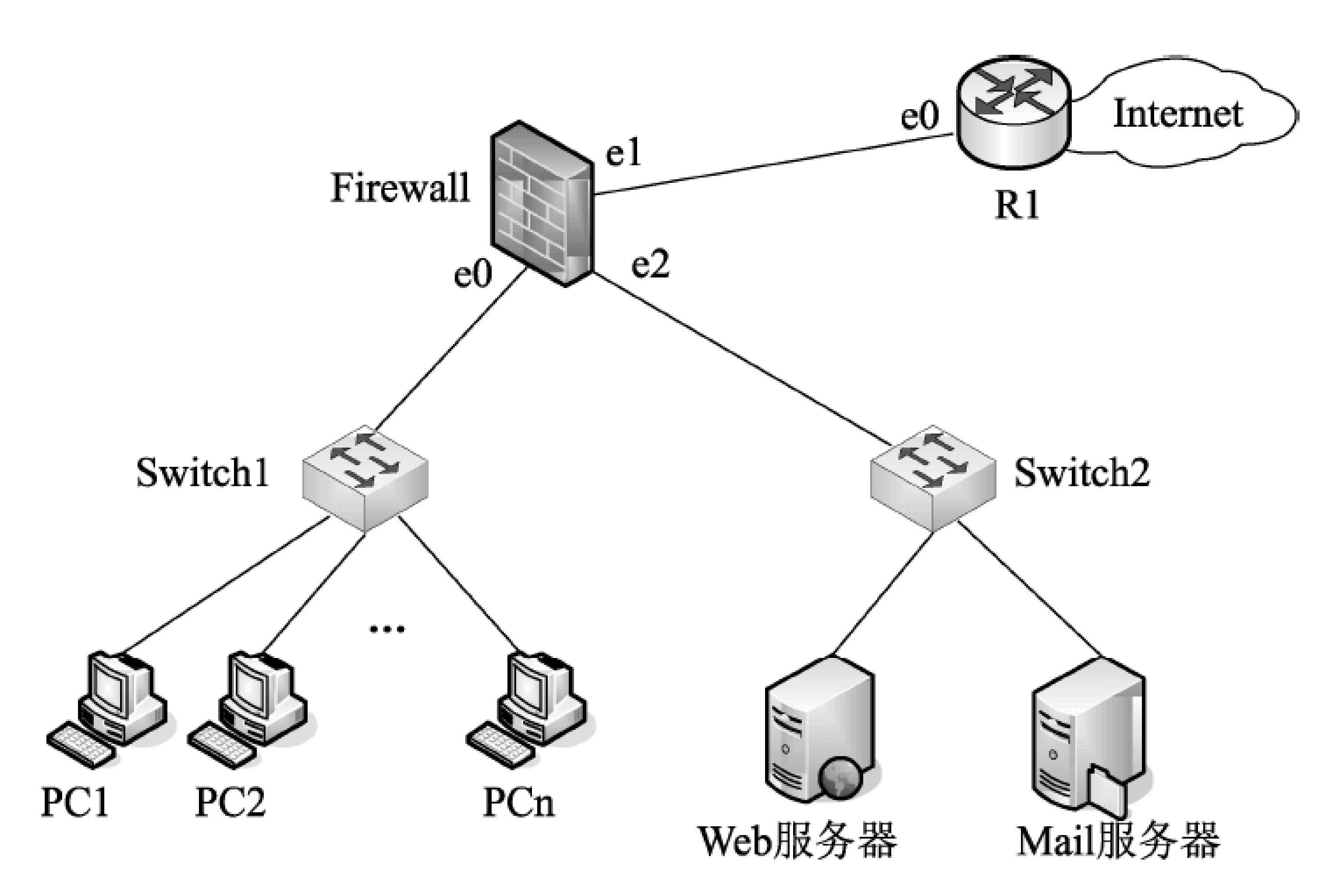



图 3-10　某公司网络拓扑结构

**【问题 3】**(3 分)

1. 对图 3-10 中主机 PC1 可分配的 IP 地址区间为__(12)__，子网掩码为__(13)__，默认网关为__(14)__。

2. PC1 主机的操作系统为 windows，在其命令行窗口输入 netstat -an，返回信息如图 3-11 所示，根据返回信息，PC1 正在请求的 Internet 服务为__(15)__，该服务与 PC1 进入通信时，PC1 所使用的源端口号的可能取值范围为__(16)__。

**【问题 4】**

图 3-10 中路由器 R1 的接口 IP 地址为__(17)__，子网掩码为__(18)__。

**分析：**

本题考查网络防火墙的使用配置。此类题目要求考生掌握基本的网络防火墙知识，同时具备基本的动手配置能力。

```
C:\netstat -an

活动连接

协议   本地地址              外部地址              状态
TCP    0.0.0.0:80            0.0.0.0:0             LISTENING
TCP    0.0.0.0:445           0.0.0.0:0             LISTENING
TCP    127.0.0.1:2001        127.0.0.1:50594       ESTABLISHED
TCP    127.0.0.4:2004        127.0.0.1:50597       ESTABLISHED
UDP    192.168.1.2:20112     124.202.163.31:53     CLOSE_WAIT
TCP    192.168.1.2:20301     202.12.250.13:80      ESTABLISHED
TCP    192.168.1.2:20302     117.110.20.32:80      ESTABLISHED
TCP    192.168.1.2:20303     218.30.250.21:80      ESTABLISHED
```

图 3-11 命令信息返回图

**【问题 1】**

本问题主要考查防火墙的工作模式。

防火墙能够工作在 3 种模式下，即路由模式、透明模式、混合模式。如果防火墙以第三层对外连接(接口具有 IP 地址)，则认为防火墙工作在路由模式下；若防火墙通过第二层对外连接(接口无 IP 地址)，则防火墙工作在透明模式下；若防火墙同时具有工作在路由模式和透明模式的接口(某些接口具有 IP 地址，某些接口无 IP 地址)，则防火墙工作在混合模式下。

**【问题 2】**

```
PIX#config terminal  //进入全局配置模式
PIX(config)#enable password cisco encry  //设置防火墙密码为cisco
PIX(config)#nameif e0 inside security 100
PIX(config)#nameif e1 outside security 0
PIX(config)#nameif e2 dmz security 50  //配置防火墙接口的名字，并指定安全级别
PIX(config)#nat (inside) 1 0 0  //表示启用nat，应用于全局地址池 1，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0
PIX(config)#static(dmz,outside) tcp 202.117.112.98 80 10.10.10.2 80 netmask 255.255.255.255 0 0  //表示 IP 地址为 10.10.10.2:80 的主机，对于通过 PIX 防火墙建立的每个会话都翻译成 202.117.112.98 这个全局地址
PIX(config)#conduit permit tcp host 202.117.112.98 eq 443 any  //允许任何外部 IP 地址对全局地址为 202.117.112.98 的主机进行 HTTPS 访问
```

**【问题 3】**

1. 本问题主要考查网络地址范围。

根据题意和防火墙配置命令可知，该子网为 192.168.1.0/24，防火墙的 e0 接口配置了 192.168.1.1 这个地址，子网掩码 255.255.255.0，且其工作在路由模式，所以可知 PC1 的地址范围为 192.168.1.2～192.168.1.254，子网掩码为 255.255.255.0，网关为 192.168.1.1。

2. 本问题主要考查考生对 netstat -an 命令的掌握和应用。

从图 3-11 可知，PC1 与外部服务器所建立的连接的端口号都为 80，因此可能正在浏览网页。PC1 所使用的源端口号从图中可以直接看出为 20301～20303。

**【问题 4】**

本问题主要考查考生对网络接口地址的配置。

从图 3-10 中可以看出，防火墙工作在路由模式，其中 el 的 IP 地址为 202.117.112.98，子网掩码为 255.255.255.252，则对端的路由器 R1 的接口 IP 地址为 202.117.112.97，子网掩码为 255.255.255.252。

答案：

【问题 1】

(1) 路由模式

(2) 透明模式

【问题 2】

(3) config terminal

(4) 设置防火墙密码

(5) inside

(6) outside

(7) dmz

(8) 表示启用 nat，应用于全局地址池 1，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0。

(9) 202.117.112.98

(10) tcp

(11) 允许任何外部 IP 地址对全局地址为 202.117.112.98 的主机进行 HTTPS 访问。

【问题 3】

(12) 192.168.1.2—192.168.1.254

(13) 255.255.255.0

(14) 192.168.1.1

(15) 访问 Web 网站

(16) 1024—65535

【问题 4】

(17) 202.117.112.98

(18) 255.255.255.252

**例 2**　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2016 年 5 月下午试题三)

【说明】

某局域网络拓扑结构如图 3-12 所示。

【问题 1】

交换机的配置方式有本地配置和远程配置两种，本地配置用配置线连接计算机的串口和交换机的__(1)__端口，通过终端仿真程序实现。远程配置通过网络采用__(2)__或 Web 实现。

【问题 2】

交换机基本配置如下，请解释配置命令。

```
//__(3)__
<quidway>system-view
//__(4)__
```

```
[Quidway]sysname NBW-S2300
 //__(5)__
[NBW-S2300]vlan batch 100 4000
 //创建 3 层接口用于管理
[NBW-S2300]interface vlanif 4000
[NBW-S2300-vlanif4000]description Manager
[NBW-S2300-vlanif4000]ip address 192.168.10.10 255.255.255.0
 //配置默认路由
[NBW-S2300]ip route-static 0.0.0.00.0.0.0 192.168.10.1
 //配置上行端口
[NBW-S2300]interface GigabitEthernet 0/0/1
[NBW-S2300-GigabitEthernet0/0/1]undo negotiation auto
[NBW-S2300-GigabitEthernet0/0/1]duplex full
[NBW-S2300-GigabitEthernet0/0/1]speed 100
[NBW-S2300-GigabitEthernet0/0/1]port link-type trunk
[NBW-S2300-GigabitEthernet0/0/1]port trunk allow-pass vlan all
 //__(6)__
[NBW-S2300-vlanif4000]interface Ethernet 0/0/1
[NBW-S2300-vlanif4000-Ethernet0/0/1]port link-type access
[NBW-S2300-vlanif4000_Ethernet0/0/1]port default vlan 100
 //创建用户，配置权限及访问类型
[NBW-S2300-vlanif4000]aaa
[NBW-S2300-vlanif4000-aaa]local-user nbw password cipher nbw 999
[NBW-S2300-vlanif4000-aaa]local-user nbw privilege level 1
[NBW-S2300-vlanif4000-aaa]local-user nbw service-type telnet terminal
 //__(7)__
[NBW-S2300-vlanif4000]super pass cipher nbw111
 //配置用户端口
[NBW-S2300-vlanif4000]user-interface vty 0 4
[NBW-S2300-vlanif4000-ui-vty0-4]authentication-mode aaa
 //__(8)__
 <NBW-S2300-vlanif4000>diaplay current-configuration
 <NBW-S2300-vlanif4000>save
```

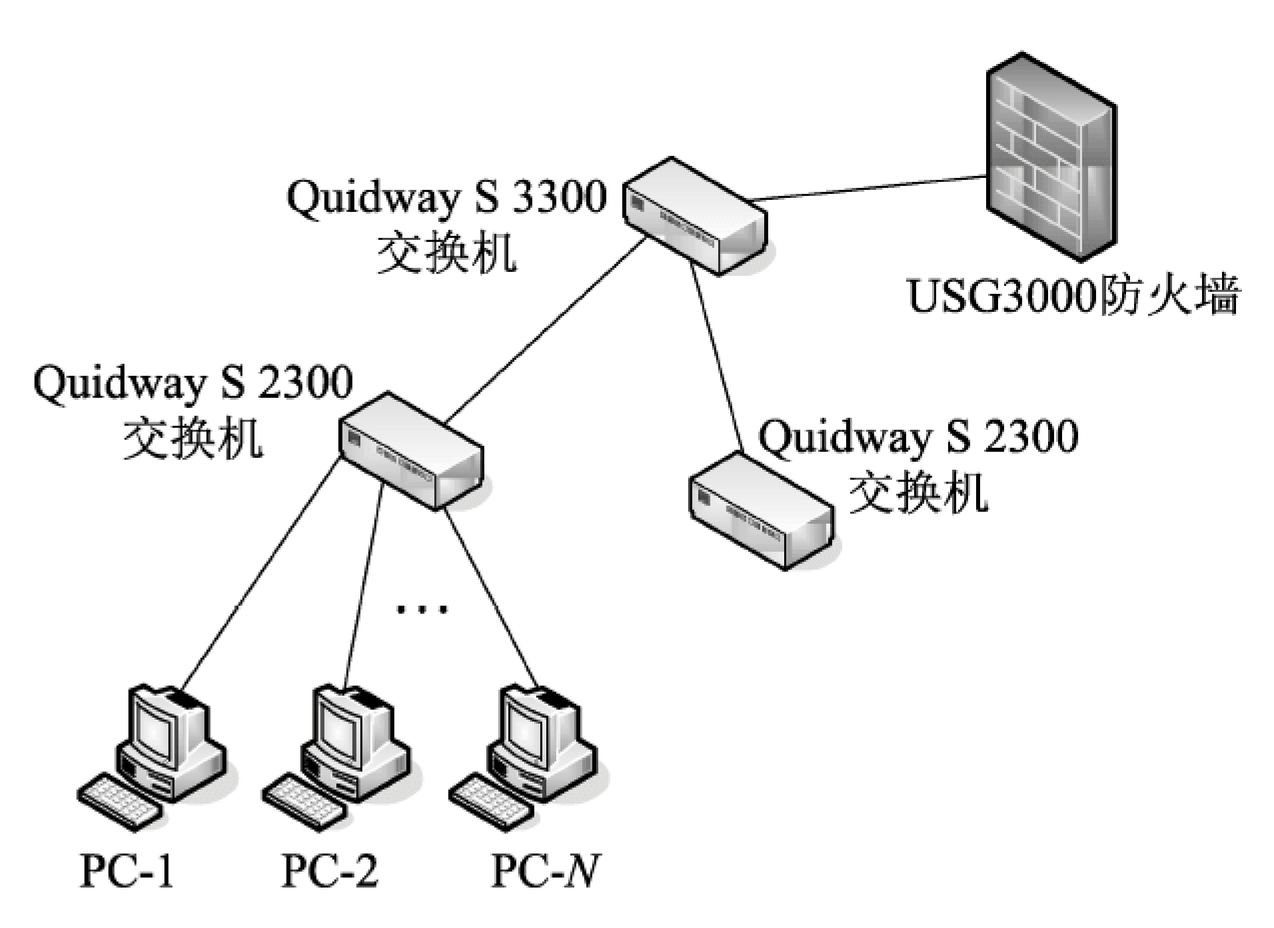



图 3-12　某公司网络拓扑结构

(3)～(8)备选答案：

A．创建管理及业务 VLAN

B．配置下行端白

C．创建 Su 密码

D．检查配置并保存

E．设备命名

F．进入配置界面

**【问题 3】**

阅读 USG3000 的配置信息，回答问题。

```
<USG3000> system-view
[USG3000] firewall mode transparent
[USG3000] firewall zone untrust
[USG3000-zone-untrust] add interface GigabitEthernet0/1
[USG3000-zone-untrust] quit
[USG3000]firewallzone trust
[USG3000-zone-trust] add interface GigabitEthernet0/0
[USG3000-zone-trust] quit
[USG3000] firewall system-ip 192.168.100.200255.255.255.0
[USG3000] firewall packet default permit all
[USG3000] firewall p2p-car default-permit
[USG3000] time_range daytime 10:00 to 24:00 daily
[USG3000] time_range night 00:00 to 10:00 daily
[USG3000] p2p-class0
[USG3000-p2p-class-0] cir 1000 index1 time-range daytime
[USG3000-p2p-class-0] cir 2000 index 2 time-range night
[USG3000-p2p-class-0] quit
```

防火墙的工作模式分为路由模式、透明模式和混合模式。该防火墙工作在__(9)__模式；上述配置信息主要是实现__(10)__；语句 time range night 00:00 to 10:00 daily 作用是__(11)__。

**【问题 4】**(3 分)

网络运行过程中出现以下现象：

(1) 随着连接数的增加，该网络逐渐变慢，一段时间后出现用户频繁掉线。

(2) 计算机重启以后网络无法连接，需要重启接入交换机接口。

(3) 网络出现丢包严重、掉线的故障，分布在不同的物理区域。

网管员在故障计算机上运行 arp-a 命令，结果如图 3-13 所示。

```
C:\>arp -a
Interface:192.168.0.112  ---0x2
  Interface Address      Physical Address      Type
  192.168.0.112          00-19-db-48-74-70     dynamic
  192.168.0.254          00-19-db-63-5b-f4     dynamic
  192.168.0.14           00-19-db-63-5b-f4     dynamic
  192.168.0.43           00-19-db-63-5b-f4     dynamic
  192.168.0.63           00-1d-92-86-d1-3e     dynamic
```

图 3-13　执行 arp-a 命令结果

请依据以上现象分析，网络出现的故障是 (12) 。解决的基本思路是 (13) 。

(13)备选答案：

A．在客户端绑定网关的 IP 和 MAC 地址

B．在客户端绑定本机的 IP 和 MAC 地址

**分析：**

**【问题 1】**在进行交换机的本地配置时，首先要实现计算机与交换机物理连接。物理连接方式是将配置电缆连接计算机的串口，一端连接交换机的“Console”口。交换机的“Console”通常位于交换机的前面板或者后面板，并在端口上有“Console”字样的标识。

在进行交换机的远程配置时，通过交换的普通端口进行连接，采用的是 Telent 远程访问协议。另一种远程配置的方式需要在本地对“Console”口初步配置 IP 信息后，通过 Web 进行交换机参数的修改并对交换机进行管理。

**【问题 2】**在对交换机进行配置时，需要对交换机的名称、密码、基本业务等内容进行设置。此类题目需要考生通过对配置文件的阅读及上下文的提示在备选答案中做出正确的选择。相关命令解释如下：

(1) vlan batch 100 4000 命令用于创建多个 VLAN。

(2) port link-type access 命令用于定义接口类型。access 表示接口只属于一个 VLAN。

(3) display current-configuration 命令用于显示当前配置信息。

**【问题 3】**网络中 Peer to Peer 流量较大时(如 BT 下载)，会影响其他业务正常进出。P2P 限流是通过对 P2P 报文的深度检测和行为检测精确地识别出网络中的 P2P 流量，并对这些流量作相应的限制。USG300 上的 P2P 限流功能通过 ACL 和设置特定时间段的限流速率的结合来限制 P2P 流量，以满足用户不同的流量控制需求。

配置信息 firewall mode transparent 指明了防火墙工作在透明模式。

**【问题 4】**网络在运行中出现故障有多方面的原因，如有设备损坏、网络病毒泛滥、网络攻击及人为操作失误等。当网络中存在多个 IP 有相同的 MAC 地址时，可以排除设备损坏和人为误操作等原因。结合测试结果和网络故障现象，可以判定该故障的主要原因是 IP 地址劫持还是伪造，网络故障现象符合 ARP 病毒的特征。

ARP 病毒主要攻击手段是路由欺骗和网关欺骗，在其发作时会向全网发送伪造的 ARP 数据包，干扰网络的运行。因此在故障处置时可以考虑通过多种方式进行 IP 与 MAC 的绑定。

**答案：**

**【问题 1】**

(1) Console 或配置　(2)Telent 或 SSH

**【问题 2】**

(3) F　(4) E　(5) A　(6) B　(7) C　(8) D

**【问题 3】**

(9) 透明　(10)P2P 限流　(11) 设置时间段 00:00—10:00

**【问题 4】**

(12) ARP 攻击　(13) A

### 3.2.3　同步练习

1. 阅读以下说明，回答问题 1 至问题 3。

**【说明】**

某公司对外提供 Web 服务及 E-mail 和 DNS 服务等，同时对所有员工提供 Internet 服务。其拓扑结构如图 3-14 所示。

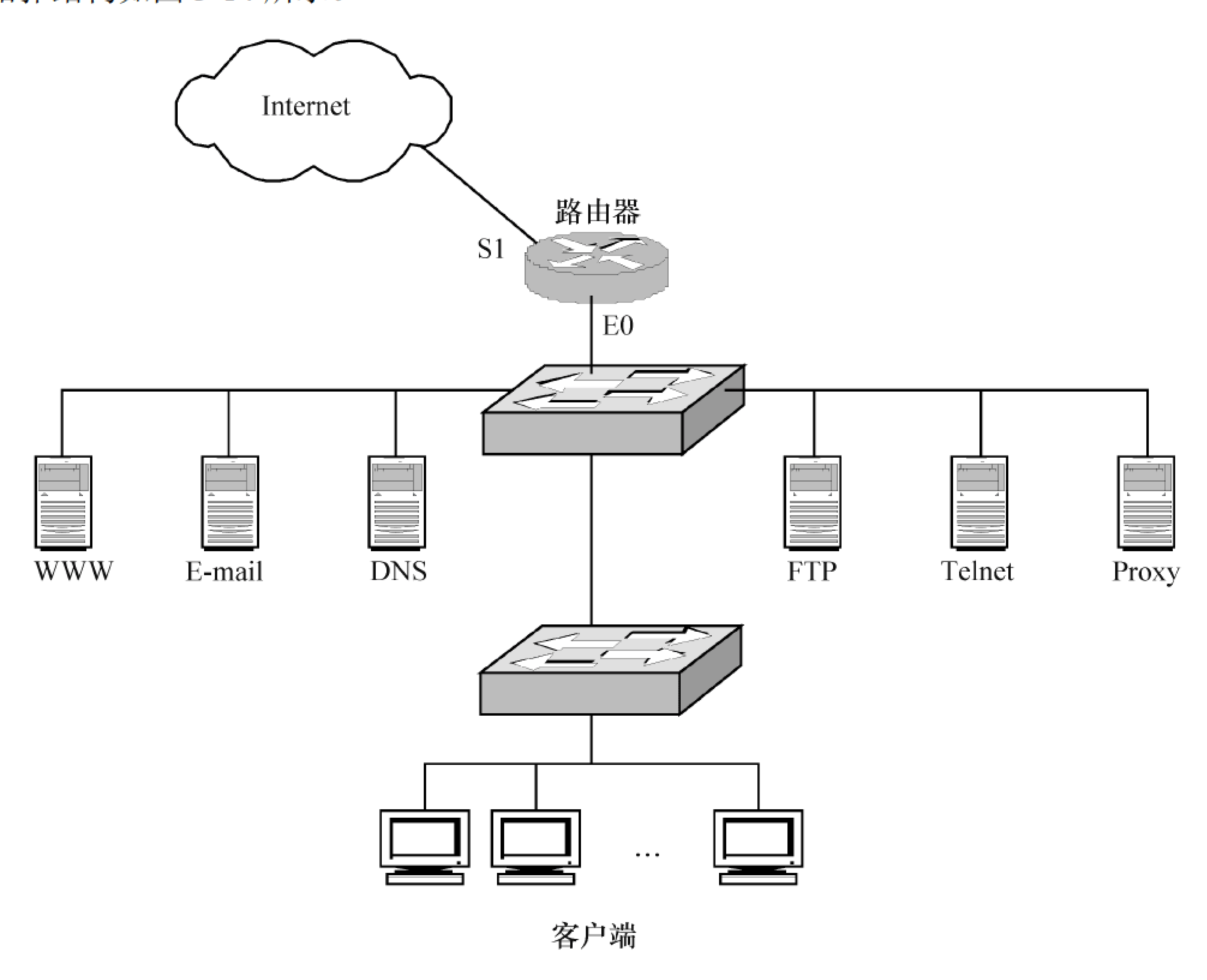



图 3-14　某公司网络拓扑结构

具体网络情况如下。

(1) 外网(即外部网)接口 S1，地址为 211.156.169.6/30(子网掩码表示由 30 个 1 组成，下同)，因特网接口端地址为 211.256.169.5/30。

(2) 内网(即内部网)接口 E0，地址为 210.45.12.1/24(可用地址空间为 210.45.12.0～210.45.12.255 这个网段，广播地址为 210.45.12.255)。

(3) 对外服务器默认网关为 210.45.12.1。

(4) 内网用户利用代理服务上网(代理服务器 IP 地址为 210.45.12.31/24)。

(5) 内网用户 IP 地址为 210.45.12.0 网段，子网掩码为 255.255.255.0，网关为 210.45.12.1，代理服务器地址为 210.45.12.31。

随着用户的增多，IP 地址紧缺的矛盾日益突出，同时内部网用户及服务器常遭受黑客的攻击。为解决上述问题，公司决定购置一台方正防火墙。

【问题 1】请给出具体方案(拓扑图)。

【问题 2】简述防火墙的硬件连接。

【问题 3】简述防火墙的配置策略。

2. 图 3-15 所示为某一公司的网络拓扑结构，请在图中标出一般用户区、公共网络、内部网络、DMZ 区、内部关键服务器群的位置。

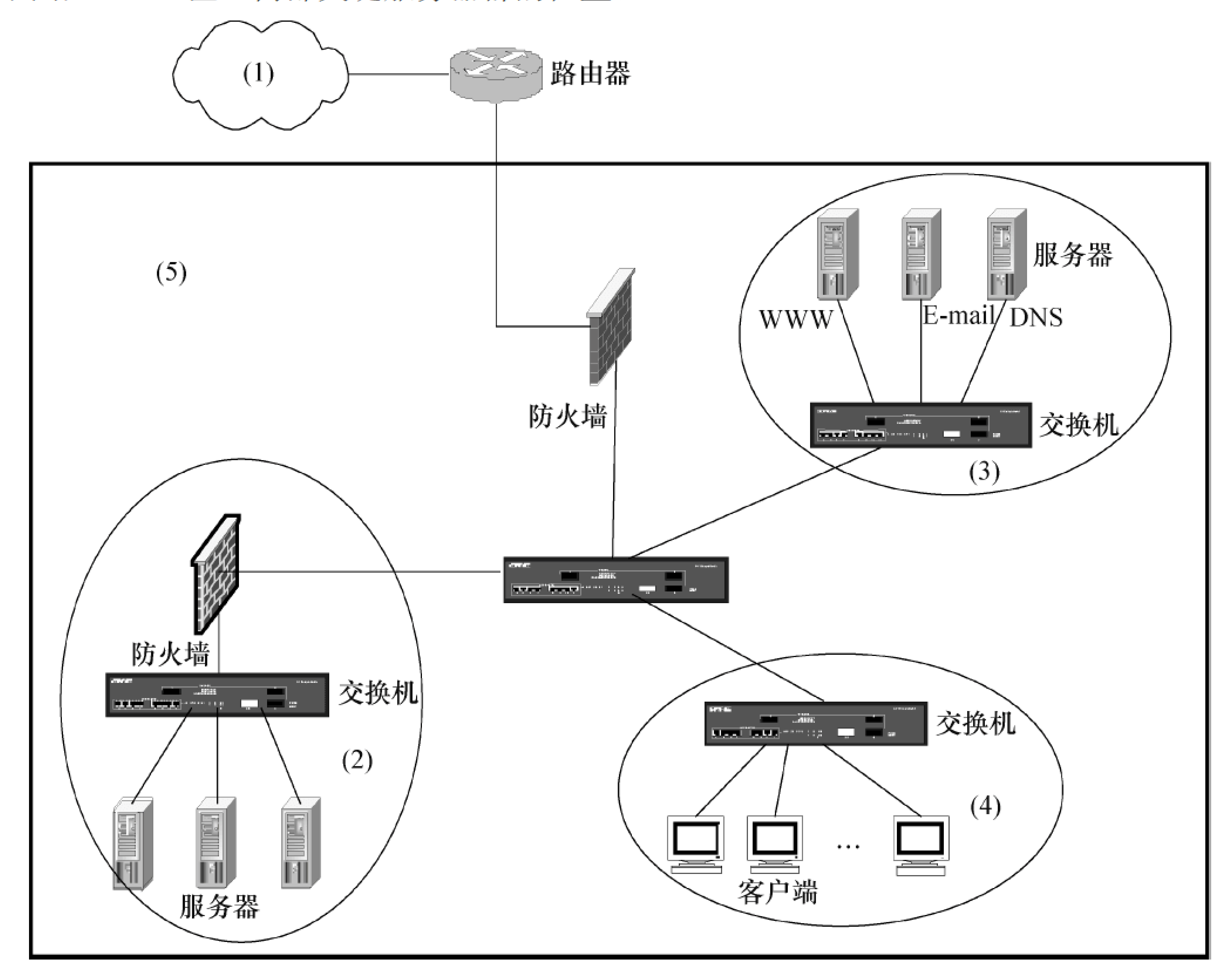



图 3-15 某公司网络拓扑结构

## 3.2.4 同步练习参考答案

1.

【问题 1】其连接拓扑结构如图 3-16 所示。

【问题 2】硬件连接如下。

(1) 用网线将路由器 E0 端口与 FireGate 的外部接口相连。

(2) 用网线将内部交换机端口与 FireGate 的内部接口相连。

(3) 用网线将 DMZ 接口与 DMZ 区交换机相连。

(4) 用电源线将 FireGate 接上电源，硬件安装完成。

【问题 3】其配置策略如下。

(1) 基本配置。

① 防火墙内部接口设为防火墙内部网络接口和管理口，地址为 192.168.1.1/24，设置

好相应的子网掩码后将其选为控制口，然后提交系统，使设备配置生效。

② 将 DMZ 区域和外网区域设置为桥，同时在桥上绑定 IP 地址 210.45.12.31/24(为原代理服务器地址)，配置完成后提交系统，使设备配置生效。

③ 添加内部网、DMZ 区域以及外部网各设备别名。

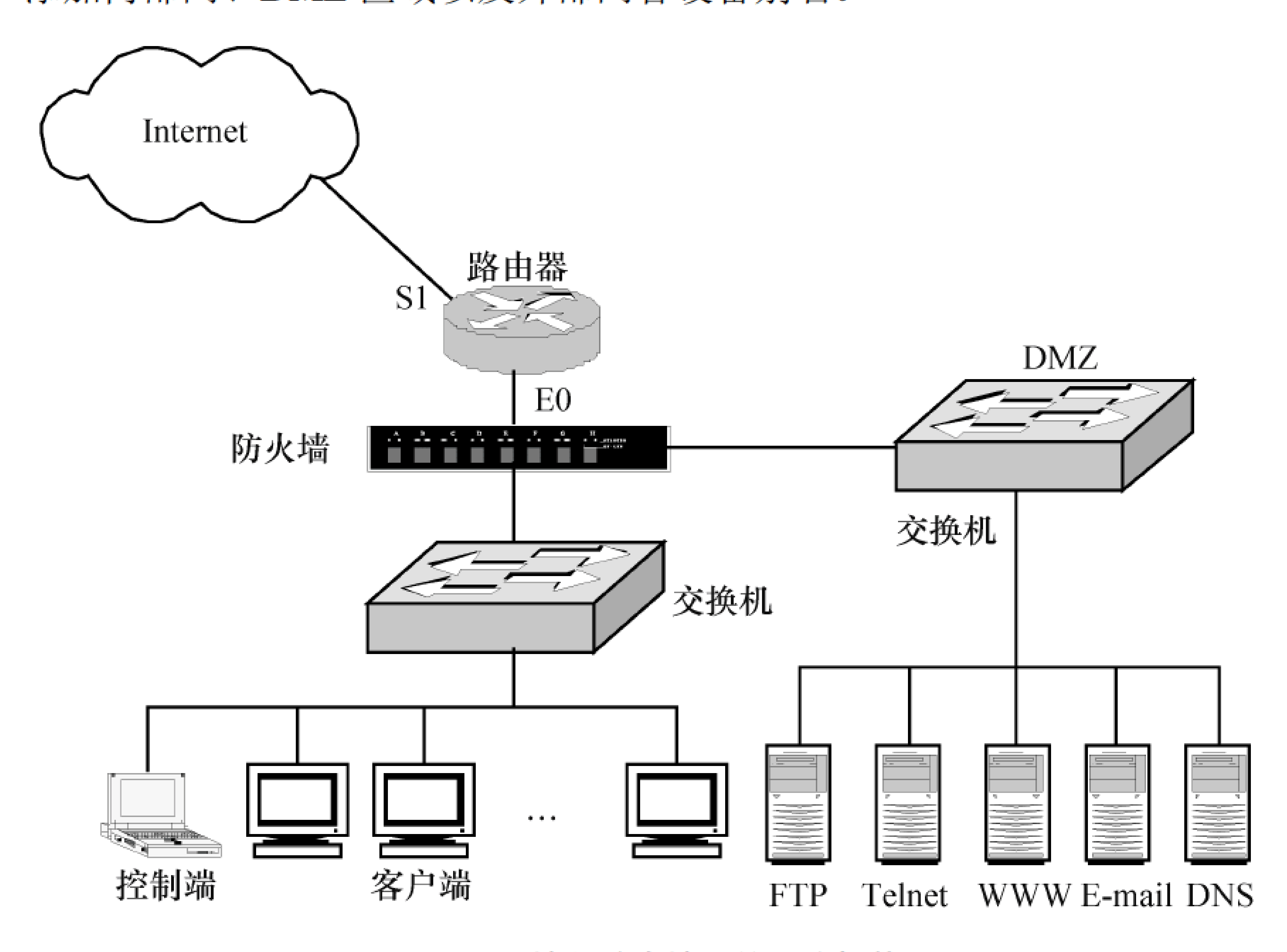



图 3-16　接入防火墙后的网络拓扑

(2) 规则配置。

① 按照实际情况配置各种安全措施，如内部网访问 DMZ 区域 Web 服务器规则、内部网访问 DMZ 区域 Telnet 服务器规则等。

② NAT 规则设置。在防火墙设置 NAT 功能实现地址转换，内部网访问外部 WWW 时，全部将内部地址转换成防火墙外部网地址 210.45.12.31，不需要代理服务器。

2.

(1) 公共网络或 Internet

(2) 内部关键服务器群区

(3) DMZ 区

(4) 一般用户区

(5) 内部网络

## 3.3　本章小结

本章知识点在 2009 年的新大纲中变化较小，主要新增了加密、认证、数字签名等安全技术知识点。

本章主要介绍了网络病毒防护策略、防火墙的配置策略、入侵处理策略。要求考生掌握网络病毒防护、防火墙、入侵处理的基本概念，熟悉在不同网络环境下的部署及网络安全解决方案。

本章内容为下午科目的重点内容，尤其是防火墙的配置，曾多次考到。

# 3.4 达标训练题及参考答案

## 3.4.1 达标训练题

阅读以下说明，回答问题 1 至问题 4。

**【说明】**

某学校的网络拓扑结构如图 3-17 所示，为加强网络安全，学校决定购置一台三端口的防火墙保护内部网络；购置了入侵检测产品对重点网段和服务器进行监控；购置一套网络版杀毒软件(Server 版)并安装于一台服务器上，客户端、服务器通过防病毒服务器提供的 Web 页面自动下载安装并具有自动跟踪防病毒服务器更新病毒库的功能。

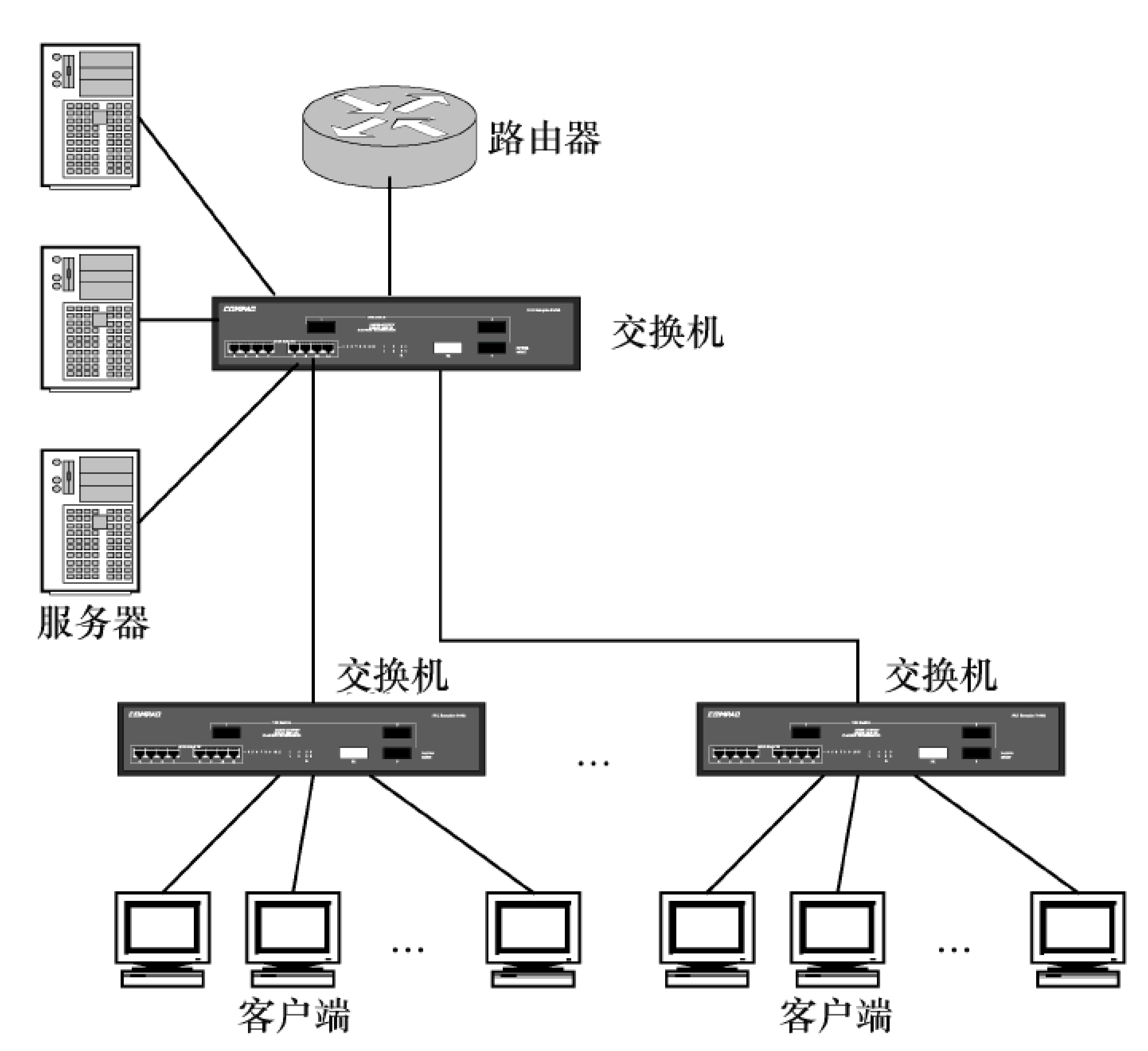



图 3-17 某校园网拓扑结构

**【问题 1】**什么是防火墙？简述其功能及优点。

**【问题 2】**什么是入侵检测？简述其功能。

**【问题 3】**什么是网络病毒？简述其特点。对防病毒服务有什么要求？

**【问题 4】**请给出该网络的安全方案(拓扑结构图)，并在图中标出相应设备的名称。

## 3.4.2　参考答案

**【问题 1】**防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，它对两个或多个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。其功能与特点如下。

(1) 对进出的数据包进行过滤，过滤掉不安全的服务和非法用户。

(2) 监视 Internet 安全，对网络攻击行为进行检测和报警。

(3) 记录通过防火墙的信息内容和活动。

(4) 控制对特殊站点的访问，封堵某些禁止的访问行为。

(5) 防火墙能强化安全策略。

(6) 防火墙能有效地记录 Internet 上的活动。

(7) 防火墙是一个安全策略的边防站。

**【问题 2】**入侵检测系统(IDS)通过从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统可以说是防火墙系统的合理补充和延伸，如果说防火墙是第一道安全闸门，入侵检测系统则可以说是第二道安全闸门。入侵检测系统在不影响网络性能的前提下，可实时、动态地保护来自内部和外部的各种攻击，同时有效地弥补了防火墙所能达到的防护极限。入侵检测系统的主要功能如下。

(1) 监测并分析用户和系统的活动。

(2) 核查系统配置和漏洞。

(3) 评估系统关键资源和数据文件的完整性。

(4) 识别已知的攻击行为。

(5) 统计分析异常行为。

(6) 进行操作系统日志管理，并识别违反安全策略的用户活动。

**【问题 3】**网络病毒是指在网络上传播的计算机病毒，可能会给网络带来灾难性后果，被称为“第二代病毒”。网络病毒的特点及危害性主要表现在破坏性强、传播性强、具有潜伏性和可激发性、针对性更强、扩展面广、传播速度快、难以彻底清除的特点。

要求防病毒服务器每天下载并更新病毒定义库。

**【问题 4】**其配置拓扑结构如图 3-18 所示。

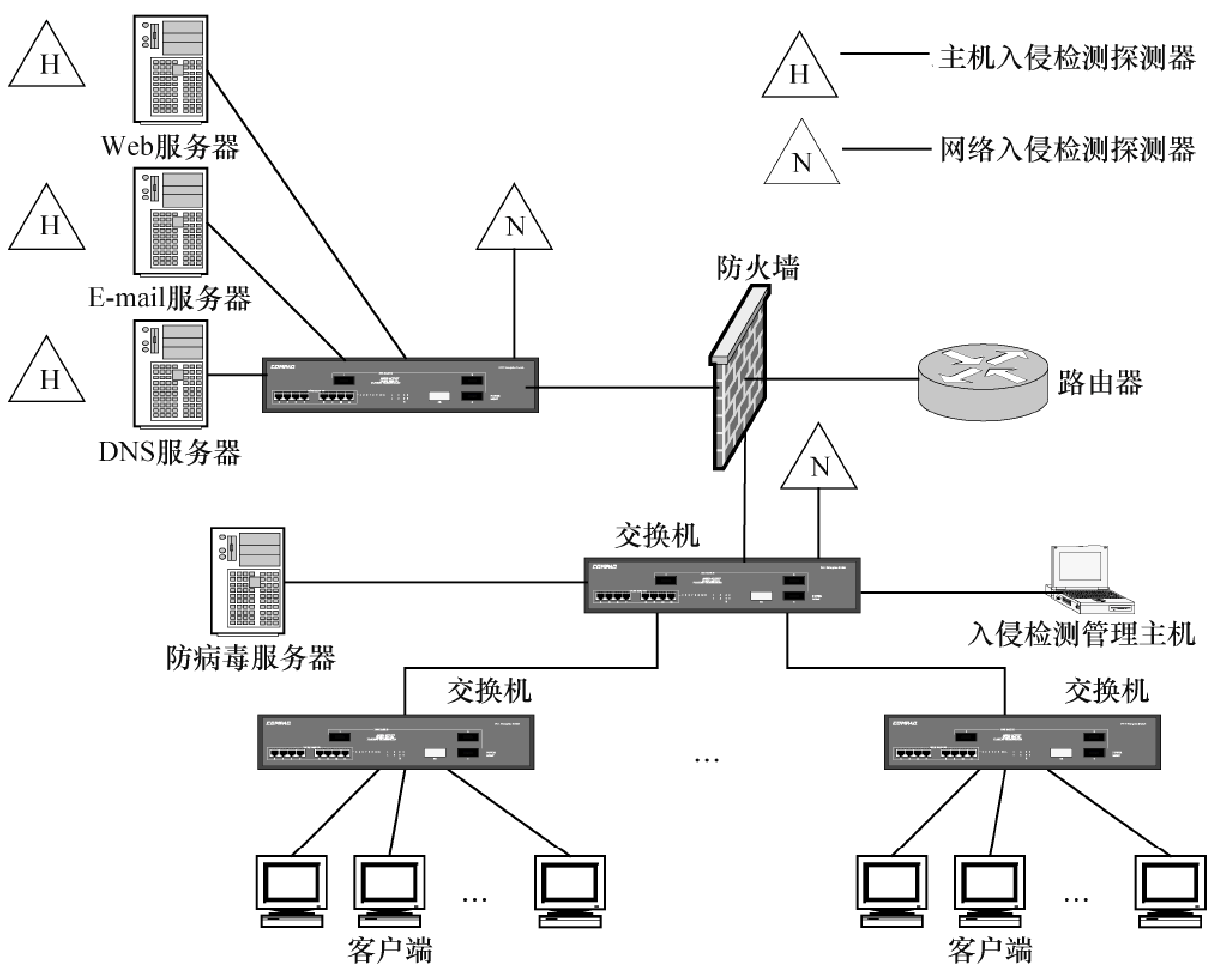



图 3-18　解决网络安全问题的拓扑结构

# 第 4 章　网络管理与故障处理

**大纲要求：**

- 使用网络管理软件对网络的配置、安全、性能、故障、计费进行监督和管理。
- 简单网络故障的分析、定位、诊断和排除。
- 小型网络的维护策略、计划和实施。
- 数据备份和数据恢复。
- 系统性能分析。

## 4.1　网络管理软件

### 4.1.1　考点辅导

#### 4.1.1.1　网络管理系统

当前能够作为管理进程运行的典型网络管理软件有惠普公司的 OpenView、IBM 公司的 NetView、SUN 公司的 SunNet 以及 Cabletron 公司的 SPECTRUM。这些网络管理系统在支持企业网络管理方案的同时，也支持通过 SNMP 对网络对象进行管理。

SNMP 操作仅支持对管理对象值的检索和修改等简单操作。具体来讲支持以下 4 种操作。

- get：用于获取特定对象的值，提取指定的网络管理信息。
- get-next：通过遍历 MIB 树获取对象的值，提供扫描 MIB 树和依次检索数据的方法。
- set：用于修改对象的值，对管理信息进行控制。
- trap：用于通报重要事件的发生，代理使用它发送非请求性通知给一个或多个预配置的管理工作站，用于向管理者报告管理对象的状态变化。

以上 4 种操作中前 3 种是由管理者发给代理请求，需要代理发出响应给管理者；最后一种则是由代理发给管理者请求，但并不需要管理者响应。

#### 4.1.1.2　TCP/IP 网络管理工具

网络管理工具有连接性测试程序(ping)、路由跟踪程序(tracert/trace/traceroute)、协议统计程序(netstat)和 MIB 变量浏览器。

1. ping：验证与远程计算机的连接

连接性测试程序就是 ping，它是一种最常见的网络工具，用这种工具可以测试端到端的连接性，即检查源端到目的端网络是否通畅。通过发送“Internet 控制报文协议(ICMP)”

回送请求/应答报文来验证与另一台 TCP/IP 计算机的 IP 级连接。

ping 的命令格式如下：

```
ping IP 地址或主机名 [-t] [-a] [-n count] [-l size]
```

其中各参数含义如下。

- -t：指定在中断前 ping 可以持续发送回响请求信息到目的端。要中断并显示统计信息，可按 Ctrl+Break 组合键；要中断并退出 ping，可按 Ctrl+C 组合键。
- -a：指定对目的端 IP 地址进行反向名称解析。如果解析成功，ping 将显示相应的主机名。
- -n count：指定发送回响请求消息的次数，具体次数由 count 来指定。若不指定次数，则默认值为 4。
- -l size：指定发送的回响请求消息中“数据”字段的长度(以字节表示)。默认值为 32。size 的最大值是 65 527B。

当计算机不能访问 Internet 时，可以首先使用 ping 命令确认是否是本地局域网的故障。假定局域网的代理服务器 IP 地址为 202.168.0.1，可使用 ping 202.168.0.1 命令查看本机是否和代理服务器连通。再测试本机的网卡是否正确安装，常用命令是 ping 127.0.0.1。

2. tracert/trace/traceroute：路由跟踪程序命令

tracert 通过递增“生存时间(TTL)”字段的值将“Internet 控制报文协议(ICMP)”回送请求/应答报文发送给目标可确定到达目标的路径。所显示的路径是源主机与目标主机间的路径中的路由器的近侧路由器接口列表。不带参数时 tracert 显示帮助。

tracert 的命令格式如下：

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

其中各参数含义如下。

- -d：指定不将地址解析为计算机名。
- -h maximum_hops：指定搜索目标的最大跃点数。
- -j computer-list：指定沿 computer-list 的稀疏源路由。
- -w timeout：每次应答等待 timeout 指定的毫秒数。
- target_name：目标计算机的名称或 IP 地址。

例如，想要了解自己的计算机与目标主机 www.cctv.com.cn 之间详细的传输路径信息，可以在 MS-DOS 方式下输入 tracert www.cctv.com.cn。

如果在 tracert 命令后面加上一些参数，还可以检测到其他更详细的信息。例如，使用参数-d，可以指定程序在跟踪主机的路径信息时也解析目标主机的域名。

3. netstat：协议统计程序

netstat 工具是用来显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议)。使用时如果不带参数，netstat 显示活动的 TCP 连接。

netstat 命令格式如下：

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

其中各参数含义如下。

- -a：显示所有连接和侦听端口。服务器连接通常不显示。
- -e：显示以太网统计。该参数可以与-s 选项结合使用。
- -n：以数字格式显示地址和端口号(而不是尝试查找名称)。
- -s：显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。
- -p protocol：显示由 protocol 指定协议的连接；protocol 可以是 TCP 或 UDP，如果与-s 选项一起使用显示每个协议的统计，则 protocol 可以是 TCP、UDP、ICMP 或 IP。
- -r：显示路由表的内容。
- interval：重新显示所选的统计，在每次显示之间暂停 interval 秒。按 Ctrl+B 组合键停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

4. MIB 变量浏览器

MIB 变量浏览器是另一种重要的网络管理工具。在 SNMP 中，MIB 变量包含了路由的几乎所有重要参数。对路由器进行管理，很大程度上是利用 MIB 变量来实现的。比如，路由器的路由表、路由器的端口流量数据、路由器中的计费数据、路由器 CPU 的温度、负载及路由器的内存余量等，所有这些数据都是从路由器的 MIB 变量中采集到的。虽然对 MIB 变量的定时采集与分析大部分都是程序进行的，但一种图形界面下的 MIB 变量浏览器也是需要的。一般 MIB 变量浏览器，都按照 MIB 变量的树形命名结构进行设计，这样就可以自顶向下，根据所要浏览的 MIB 变量的类别逐步找到该变量，而无须记住该变量复杂的名字。网络管理人员可以利用 MIB 变量浏览器取出路由器当前的配置信息、性能参数以及统计数据等，对网络情况进行监控。

Microsoft 提供了一个实用程序 Snmputil，可以用于测试 SNMP 服务，也可以用于测试用户开发的扩展代理。

Snmputil 的用法如下：

```
Snmputil [get|getnext|walk] agentaddress community old[old…]
Snmputil trap
```

可以使用 Snmputil 发送 GetRequest 或 GetNextRequest 报文，也可以用 Snmputil 遍历整个 MIB 子树。一种较好的测试方法是同时打开两个 DOS 窗口，在一个窗口中用 Snmputil 发送请求，在另一个窗口中用 Snmputil 接收异常报告情况。

## 4.1.2　典型例题分析

**例 1**　某一大型园区网，由若干个路由器构成园区网主干。有两台 Windows 2000 主机无法正常通信，怀疑是其中某个路由器工作不正确或配置错误而引起的，网络管理员应用什么命令来找到这个路由器？

**分析**：该题主要考查考生对 tracert 命令的使用和掌握情况。

在 Windows 2000 中提供了一个跟踪程序命令 tracert 可以跟踪数据包经过的路由。该工具将包含不同生存时间(TTL)值的 Internet 控制消息协议(ICMP)回显数据包发送到目标主机，以决定到达目标主机所经历的路由器。由于要求路径上的每个路由器在转发数据包之前至少将 IP 数据包中的 TTL 递减 1，所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息送回源主机。路由跟踪程序先发送 TTL 为 1 的回显数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定数据包经过的路由器。如果检查出到哪个路由器之前都能正常响应，到某一个路由器就不能响应了，这样就很容易知道如果线路出现故障，故障点就可能出在某处。

**答案**：tracert <目的主机的 IP 地址或域名>

**例 2** 为了分析一台安装了 Windows Server 2003 服务器的网络流量，使用查看网络状态信息工具 netstat。如果想每 30 秒统计一下 TCP 连接情况，该使用哪些参数？(写出完整命令)

**分析**：该题主要考查考生对 netstat 命令使用掌握情况。

netstat 命令可以帮助网络管理员了解网络的整体使用情况。它既可以显示当前正在活动的网络连接的详细信息，如显示网络连接、路由表和网络接口信息，也可以统计目前总共有哪些网络连接正在运行。其命令格式如下：

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

其中，参数-p protocol 用于显示指定协议的网络连接；参数-s 用于显示每个协议的统计；参数 interval 设定重新显示所选统计的间隔时间。因此命令为：

```
netstat -s -p TCP 30
```

**答案**：netstat- s - p TCP 30

## 4.1.3 同步练习

1．命令“ping 210.45.40.1-t-l 512”的含义是什么？

2．命令“tracert-h 10-w 50 210.45.40.1”的含义是什么？

3．为了分析一台安装了 Windows Server 2003 服务器的网络流量，使用查看网络状态信息工具 netstat。如果想每 30 秒显示一下 UDP 连接情况并进行统计，该使用哪些参数？(写出完整命令)

4．某台安装了 Windows Server 2003 服务器的网络装有多块网卡，不同网卡接入了不同网络，管理员通过 Windows Server 2003 中的 route 命令增加了路由表，那么使用什么命令来查看这个路由表呢？

## 4.1.4 同步练习参考答案

1．连续向 IP 地址为 210.45.40.1 的主机发送大小为 512B 的数据包，以检查该主机是否

返回这些数据包的响应。

2．查看数据包从本地主机到 IP 地址为 210.45.40.1 的主机所经过的路由，最大跃点数为 10，等待时间为 50ms。

3．netstat　-s -p udp 30

4．netstat -r

# 4.2 网 络 故 障

## 4.2.1 考点辅导

### 4.2.1.1 网络故障诊断与排除的基本概念

网络故障诊断是以网络原理、网络配置和网络运行的知识为基础，从故障现象出发，以网络诊断工具为手段获取诊断信息、确定网络故障点、查找问题的根源、排除故障、恢复网络正常运行的软件或者硬件。网络故障通常有以下几种可能。

(1) 物理层中物理设备相互连接失败或者硬件及线路本身的问题。

(2) 数据链路层网络设备的接口配置问题。

(3) 网络层网络协议配置或操作错误。

(4) 传输层设备性能或通信拥塞的问题。

(5) 上三层或网络应用程序错误。

网络故障的诊断过程应该沿着 OSI 七层模型从物理层开始向上进行。首先检查物理层，然后检查数据链路层，以此类推，设法确定通信失败的故障点，直到系统通信正常为止。

网络诊断可以使用包括局域网或广域网分析仪在内的多种工具，包括路由器诊断命令、网络管理工具和其他故障诊断工具。一般情况下，查看路由表是解决网络故障时的首选。ICMP 的 ping、trace 命令及 Cisco 的 show 命令、debug 命令是获取故障诊断有用信息的网络工具。通常使用一个或多个命令收集相应的信息，在给定情况下确定使用什么命令获取所需要的信息。

网络故障往往以某种症状表现出来，对每一个症状使用特定的故障诊断工具和方法都能查找出一个或多个故障原因。

### 4.2.1.2 网络故障的分类

根据网络故障的性质把网络故障分为物理故障(硬件故障)与逻辑故障(软件故障)，也可以根据网络故障的对象把网络故障分为线路故障、路由器故障和主机故障。

1．按网络故障的性质分类

首先介绍按照网络故障的不同性质而划分的物理故障(硬件故障)与逻辑故障(软件故障)。

1) 物理故障

物理故障指的是设备或线路损坏、插头松动、线路受到严重电磁干扰等情况。

2) 逻辑故障

逻辑故障中最常见的情况就是配置错误，指由于网络主机或网络设备的配置原因而导

致的网络异常或故障。配置错误可能是主机、交换机或路由器端口参数设定有误，或路由器路由配置错误以至于路由循环或找不到远端地址，或者是路由掩码设置错误等。比如，同样是网络中的线路故障，该线路没有流量，但又可以 ping 通线路的两端端口，这时就很有可能是路由配置错误了。遇到这种情况，通常用“路由跟踪程序”(在不同系统中的路由跟踪命令并不相同，在 Windows 环境下使用 tracert 命令，在 Linux 或 UNIX 下使用 traceroute 命令，在 Cisco 路由器中使用 trace 命令)，它和 ping 命令类似，最大的区别在于路由跟踪程序是把端到端的线路按线路所经过的路由器分成多段，然后以每段返回响应与延迟。如果发现在路由跟踪程序的结果中某一段之后，两个 IP 地址循环出现，这时，一般就是线路远端把端口路由又指向了线路的近端，导致 IP 数据包在该线路上来回反复传递。这时只需更改远端路由器端口配置，就能恢复线路正常。

逻辑故障的另一类情况就是一些重要进程或端口关闭及系统的负载过高。如也是线路中断，没有流量，用 ping 发现线路端口不通，检查发现该端口处于 down 的状态，这就说明该端口已经关闭，因此导致故障。这时只需重新启动该端口，就可以恢复线路的连通了。还有一种常见的故障情况是路由器的负载过高，表现为路由器 CPU 温度太高、CPU 利用率太高及内存剩余太少等，如果因此影响网络服务质量，最直接也是最好的办法就是更换路由器，当然要换个好点的。

2. 按网络故障发生地址分类

网络故障根据故障的不同对象也可以划分为线路故障、路由器故障和主机故障。

1) 线路故障

线路故障最常见的情况就是线路不通。诊断这种情况首先应检查该线路上流量是否还存在，然后用 ping 检查线路远端的路由器端口能否响应，用 traceroute 检查路由器配置是否正确，找出问题逐个解决。

2) 路由器故障

线路故障中很多情况都涉及路由器，因此也可以把一些线路故障归结为路由器故障。检测路由器故障需要利用 MIB 变量浏览器，用它收集路由器的路由表、端口流量数据、计费数据、路由器 CPU 的温度、负载以及路由器的内存剩余量等数据。通常情况下，网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。

3) 主机故障

主机故障常见的现象就是主机的配置不当。如主机配置的 IP 地址与其他主机冲突，或 IP 地址根本就不在子网范围内，由此导致主机无法连通。主机的另一常见故障就是安全故障。

### 4.2.1.3 网络故障的分层诊断技术

1. 物理层及其诊断

物理层是 OSI 分层结构体系中最基础的一层，它建立在通信媒体的基础上，是系统和通信媒体的物理接口，为数据链路实体之间进行透明传输，为建立、保持和拆除计算机和网络之间的物理连接提供服务。物理层的故障主要表现在设备的物理连接方式不恰当及连接电缆不正确。确定路由器端口物理连接是否完好的最佳方法是使用 show interface 命令，检查每个端口的状态，解释屏幕输出信息，查看端口状态、协议建立状态和 EIA 状态。

2. 数据链路层及其诊断

数据链路层的主要任务是使网络层无须了解物理层的特征而获得可靠的传输。数据链路层为通过链路层的数据进行封装和拆封装、差错检测和一定程度的校正，并协调共享介质。查找和排除数据链路层的故障，需要查看路由器的配置。

3. 网络层及其诊断

网络层提供建立、保持和释放网络层连接的手段，包括路由选择、流量控制、传输确认、中断、差错及故障恢复等。排除网络层故障的基本方法是沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的 IP 地址。如果路由没有在路由表中出现，应该通过检查来确定是否已经输入适当的静态路由、默认路由或者动态路由，然后手工配置一些丢失的路由，或者排除一些动态路由选择过程的故障。

#### 4.2.1.4　局域网常见故障的排除

虽然网络故障原因多种多样，但总的来讲不外乎硬件问题和软件问题，说得再确切一些，这些问题就是网络连接性故障、网络协议故障和网络配置故障。

1. 网络连接性故障

故障发生后，首先应当考虑的是网络连接性问题。连接性的问题通常涉及网卡、跳线、信息插座、网线、Hub、交换机、Modem 等设备和通信介质，其中任何一个设备的损坏都会导致网络连接的中断。连接性通常可采用软件和硬件工具进行测试验证。例如，当某台计算机不能浏览 Web 时，在网络管理员的脑子中产生的第一个想法就是网络连接性的问题。到底是不是呢？可以通过测试进行验证。看得到网上邻居吗？可以收发电子邮件吗？ping 得通网络内的其他计算机吗？只要其中一项回答为“是”，那就可以断定本机到 Hub 或交换机的连接性没有问题。当然，即使都回答“否”，也不就表明连接性肯定有问题，而是可能会有问题，因为如果计算机的网络协议的配置出现了问题也会导致上述现象的发生。另外，看一看网卡和 Hub 或交换机接口上的指示灯是否闪烁及闪烁是否正常也是个不错的主意。

排除了由于计算机网络协议配置不当而导致故障的可能后，就应该查看网卡和 Hub 的指示灯是否正常、测量网线是否畅通。

1)　故障表现

连接性故障通常表现为以下几种情况。

(1)　计算机无法登录到服务器。

(2)　计算机无法通过局域网接入 Internet。

(3)　计算机在“网上邻居”中只能看到自己，而看不到其他计算机，从而无法使用其他计算机上的共享资源和共享打印机。

(4)　计算机无法在网络内实现访问其他计算机上的资源。

(5)　网络中的部分计算机运行速度异常缓慢。

2)　故障原因

以下原因可能导致连接性故障。

(1)　网卡未安装或未安装正确，或与其他设备有冲突。

(2)　网卡硬件故障。

(3) 网络协议未安装或设置不正确。

(4) 网线、跳线或信息插座故障。

(5) Hub 或交换机电源未打开，Hub 或交换机硬件故障，Hub 或交换机端口硬件故障。

(6) UPS 电源故障。

3) 故障排除方法

(1) 确认连接性故障。当出现一种网络应用故障，如无法接入 Internet 时，首先尝试使用其他网络应用，如查找网络中的其他计算机或使用局域网中的 Web 浏览等。如果其他网络应用可正常使用，如虽然无法接入 Internet，却能够在“网上邻居”中找到其他计算机，则可 ping 通其他计算机，即可排除连接性故障。如果其他网络应用均无法实现，则继续下面的操作。

(2) 看 LED 灯判断网卡的故障。首先查看网卡的指示灯是否正常。正常情况下，在不传送数据时，网卡的指示灯闪烁较慢，传送数据时闪烁较快。如果是不亮，或者是长亮不灭，都表明有故障存在。如果网卡的指示灯不正常，需关掉计算机更换网卡。对于 Hub 或交换机的指示灯，凡是插有网线的端口指示灯都亮。Hub 指示灯的作用只能指示该端口是否连接有终端设备，而不能显示通信状态。有的交换机指示灯则通过不同的颜色来表示不同的通信状态，如用绿色表示正常通信、用橙色表示阻断通信。

(3) 用 ping 命令排除网卡故障。使用 ping 命令，ping 本地的 IP 地址或主机名(如 server01)，检查网卡和 IP 网络协议是否安装完好。如果能 ping 通，说明该计算机的网卡和网络协议设置都没有问题，问题出在计算机与网络的连接上。因此，应当检查网线和 Hub(或交换机)的接口状态，如果无法 ping 通，只能说明 TCP/IP 协议有问题，这时可以在计算机的“控制面板”的“系统”中查看网卡是否已经安装或是否出错。如果在系统中的硬件列表中没有发现网络适配器，或网络适配器前方有一个黄色的“!”，说明网卡未安装正确，需将未知设备或带有黄色“!”的网络适配器删除。刷新后重新安装网卡，并为该网卡正确安装配置网络协议，然后进行应用测试。如果网卡无法正确安装，说明网卡可能损坏，必须换一块网卡重试。如果网卡安装正确，则故障原因是协议未安装。

(4) 如果确定在网卡和协议都正确的情况下网络还是不通，可以初步断定是 Hub(或交换机)和双绞线的问题。为了进一步确认，可再换一台主机用同样的方法进行判断。如果其他计算机与本机连接正常，则故障一定在先前那台主机和 Hub(或交换机)的接口上。

(5) 如果确定 Hub(或交换机)有故障，应首先检查 Hub(或交换机)的指示灯是否正常，如果先前那台计算机与 Hub(或交换机)连接的接口灯不亮，说明该 Hub(或交换机)的接口有故障。

(6) 如果 Hub(或交换机)没有问题，则检查计算机到 Hub 的那一段双绞线和所安装的网卡是否有故障。判断双绞线是否有问题可以通过双绞线测试仪或用两块三用表分别由两个人在双绞线的两端测试。主要测试双绞线的 1、2 和 3、6 四条线(其中 1、2 线用于发送，3、6 线用于接收)。如果发现有一根不通就要重新制作。

通过上面的操作就可以判断故障是否出在网卡、双绞线或 Hub(或交换机)上，从而将故障一一予以排除。

2. 网络协议故障

没有网络协议，网络设备和计算机之间就无法实现通信，不能实现资源共享。

1)　协议故障的表现

协议故障通常表现为以下几种情况。

(1)　计算机无法登录到服务器。

(2)　计算机在“网上邻居”中既看不到自己，也无法在网络中访问其他计算机。

(3)　计算机在“网上邻居”中能看到自己和其他成员，但无法访问其他计算机。

(4)　计算机无法通过局域网接入 Internet。

2)　故障原因分析

(1)　协议未安装。实现局域网通信，需安装 NetBEUI 协议，这有助于提高网络速度。

(2)　协议配置不正确。TCP/IP 协议涉及的基本参数有 4 个，包括 IP 地址、子网掩码、DNS 和网关，任何一个设置错误都会导致故障发生。

3)　排除步骤

当计算机出现以上协议故障现象时，应当按照以下步骤进行故障的定位。

(1)　检查计算机是否安装 TCP/IP 和 NetBEUI 协议，如果没有，建议安装这两个协议，并把 TCP/IP 参数配置好，然后重新启动计算机。

(2)　使用 ping 命令，测试与其他计算机的连接情况。

(3)　在“控制面板”的“网络”属性中单击“文件及打印共享”按钮，在打开的“文件及打印共享”对话框中检查一下，看看是否选中了“允许其他用户访问我的文件”和“允许其他电脑使用我的打印机”复选框，或者选中其中的一个。如果都没有选中，则应全部选中或选中其中一个；否则将无法使用共享文件夹。

(4)　系统重新启动后，双击“网上邻居”图标，将显示网络中的其他计算机和共享资源。如果仍看不到其他计算机，可以使用“查找”命令找到其他计算机。

(5)　在“网络”属性的“标识”中重新为该计算机命名，使其在网络中具有唯一性。

### 3.　网络配置故障

配置错误也是导致故障发生的重要原因之一。服务器、工作站、交换机、路由器都有自己的配置选项，如果网络管理员对服务器、交换机、路由器等有不当设置就会导致网络故障。例如，对服务器权限的设置不当，会导致资源无法共享的故障。计算机的使用者对计算机设置的修改，也往往会产生一些令人意想不到的访问错误，如网卡配置不当会导致无法连接的故障。

1)　故障表现及分析

配置故障更多地表现在不能实现网络所提供的各种服务上，如不能访问某一台计算机等。因此，在修改配置前必须做好原有配置的记录，并且最好进行备份。

配置故障通常表现为以下两种。

(1)　计算机只能与某些计算机而不是全部计算机进行通信。

(2)　计算机无法访问任何其他设备。

2)　配置故障排除步骤

首先检查发生故障计算机的相关配置。如果发现错误并修改后，再测试相应的网络服务能否实现。如果没有发现错误，或相应的网络服务不能实现，可执行下述步骤。

测试系统内的其他计算机是否有类似的故障，如果有同样的故障，说明问题出在网络设备上，如 Hub 或交换机；反之，检查被访问计算机对该计算机所提供的服务。

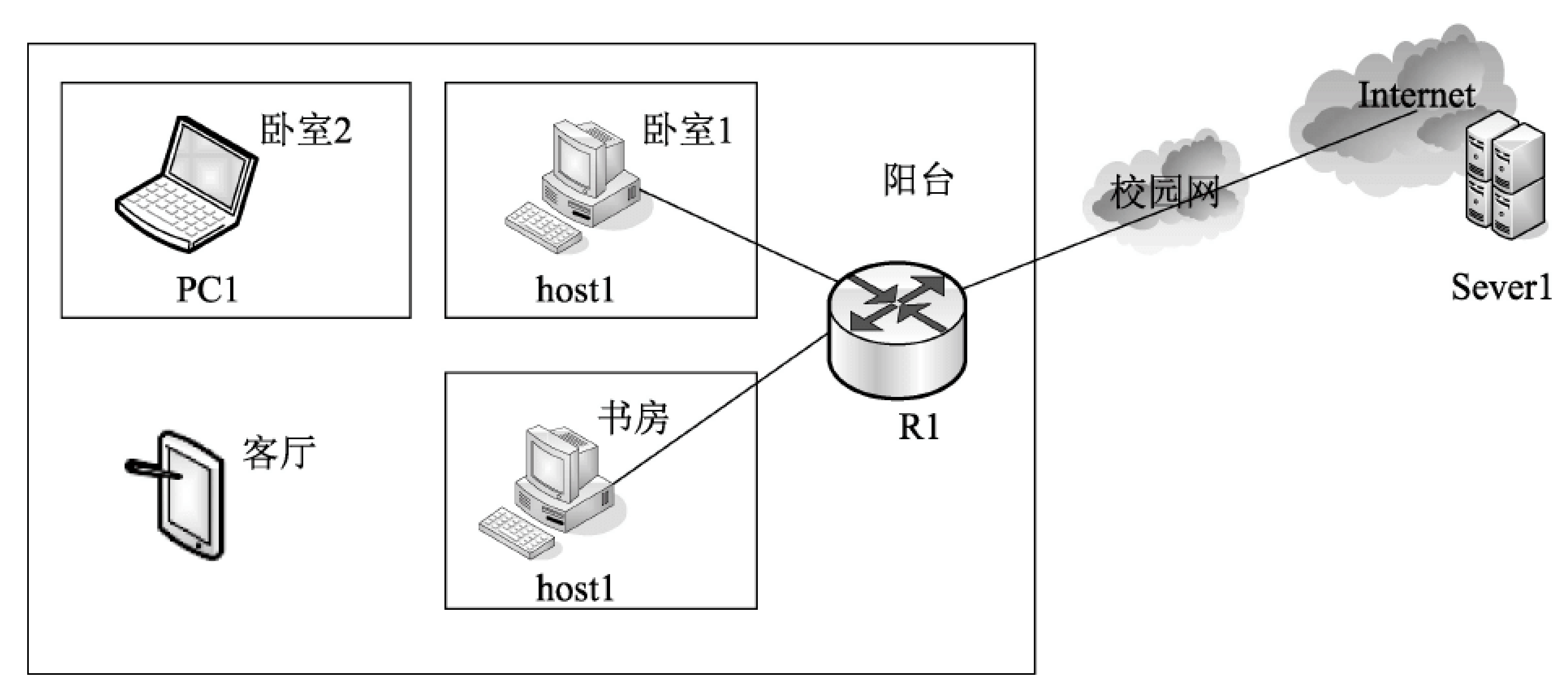
网络故障虽然多种多样，但并非无规律可循。随着理论知识和经验技术的积累，故障排除将变得越来越快、越来越简单。严格的网络管理是减少网络故障的重要手段；完善的技术档案是排除故障的重要参考；有效的测试和监控工具则是预防、排除故障的有力助手。

## 4.2.2　典型例题分析

**例 1**　阅读以下说明，回答问题 1 至问题 7，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题一)

**【说明】**

某家庭采用家庭路由器接入校园网，如图 4-1 所示。在路由器 R1 上配置有线和无线连接功能，部分配置信息如图 4-1 所示。




LAN 口状态

| | |
|---|---|
| MAC 地址： | 28-2C-B2-82-AF-28 |
| IP 地址： | 192.168.1.1 |
| 子网掩码： | 255.255.255.0 |

无线状态

| | |
|---|---|
| 无线功能： | 启用 |
| SSID 号： | FAST_8888 |
| 信　道： | 自动（当前信道 1） |
| 模式： | 11bgn mixed |
| 频段带宽： | 自动 |
| MAC 地址： | 28-2C-B2-82-AF-28 |
| WDS 状态： | 未开启 |

WAN 口状态

| | |
|---|---|
| MAC 地址： | 28-2C-B2-82-AF-29 |
| IP 地址： | 10.169.247.64 |
| 子网掩码： | 255.255.255.0 |
| 网关： | 10.169.247.254 |
| DNS 服务器： | 202.110.112.3 , 221.10.1.67 |
| 上网时间： | 0 day（s）　20：48：14 |

图 4-1　某家庭网络拓扑结构及配置信息

**【问题 1】**(4 分)

该家庭网络中有线网络采用__(1)__型拓扑结构。

**【问题 2】**(4 分)

路由器 R1 有 6 个 LAN 和一个 WAN 接口，和校园网链接的是接口__(2)__，host1 连接的是接口__(3)__。

**【问题 3】**(3 分)

在 host1 上如何登录 R1 的配置界面?

**【问题 4】**(2 分)

某主机 host1 采用静态口地址配置，其“Internet 协议版本 4(TCP/IPv4)属性”参数如图 4-2 所示，请填写 host1 的 Internet 协议属性参数。

IP 地址：__(4)__；

子网掩码：__(5)__；

默认网关：__(6)__。

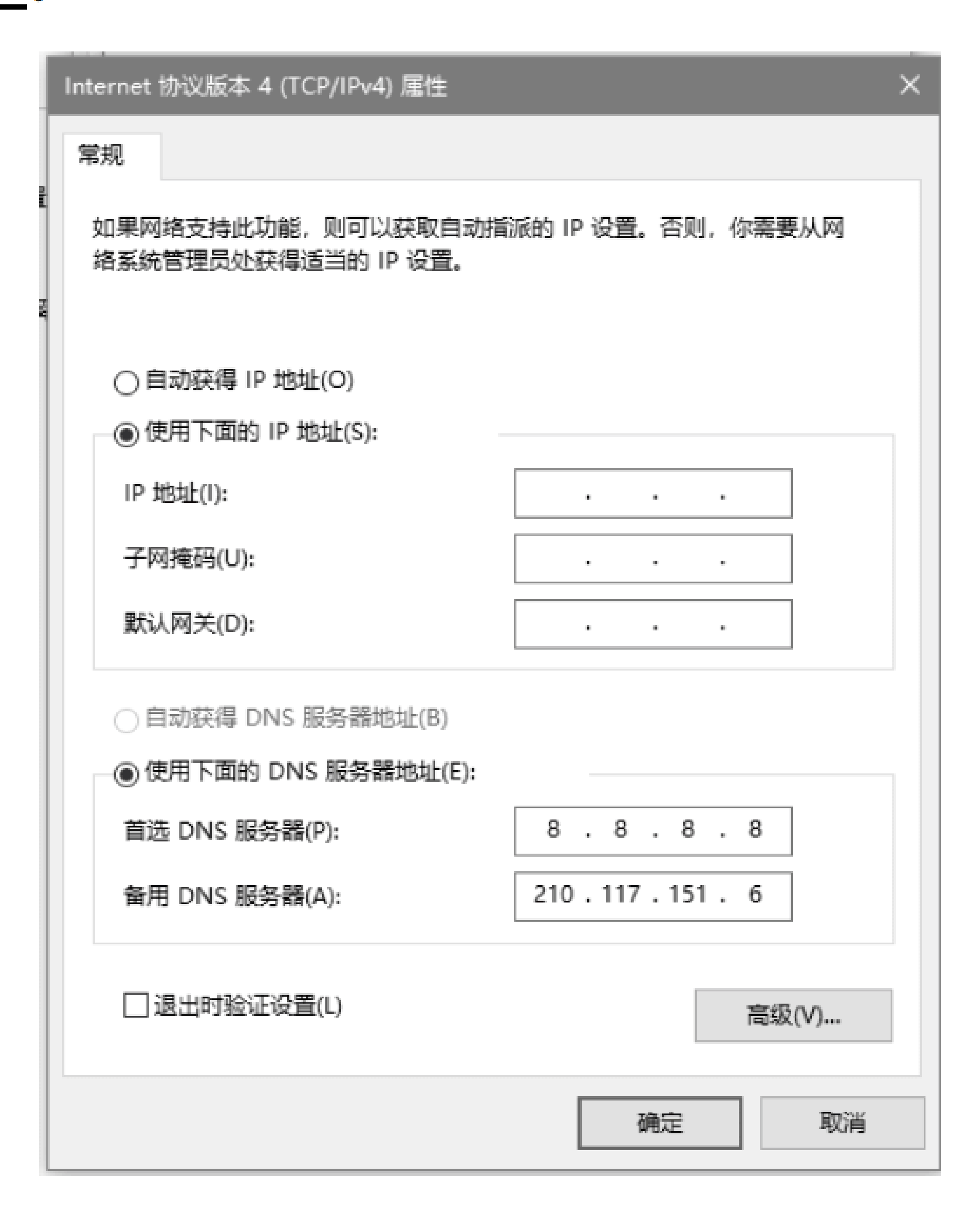



图 4-2　“Internet 协议版本 4(TCP/IPv4)属性”参数

**【问题 5】** (2 分)

为了使手机、PAD 等移动设备能自动获取 IP 地址，路由器上须开启__(7)__功能，路由器的“无线网络基本设置”界面如图 4-3 所示，SSID 为__(8)__。

WPA2-PSK 采用的加密算法为__(9)__。

(9) 备选答案：

A．AES　　B．TKIP　　C．WEP

**【问题 6】**

校园网提供的 IP 地址为__(10)__。

无线网络基本设置

本页面设置路由器无线网络的基本参数。

SSID号：
信道：4
模式：11bgn mixed
频段带宽：20MHz
☑ 开启安全设置
安全类型：WPA-PSK/WPA2-PSK
安全选项：WPA-PSK

图 4-3 “无线网络基本设置”界面

【问题 7】

PC1 访问 Internet 资源 Server1 时，在上行过程中至少应做__(11)__次 NAT 变换。

路由器 R1 上的 NAT 表如表 4-1 所示，PC1 访问 Internet 时经过 R1 后的报文 IP 地址如表 4-2 所示，则 PC1 的 IP 地址为__(12)__。Server1 的 IP 地址为__(13)__。

表 4-1 路由器 R1 上的 NAT 表

| R1 NAT 变换表 | |
|---|---|
| 内部 IP/端口号 | 变换后的端口号 |
| 192.168.1.3:1358 | 34576 |
| 192.168.1.2:1252 | 65534 |
| 192.168.1.5:1252 | 20000 |

表 4-2 PCI 访问 Internet 时经过 R1 后的报文 IP 地址

| 源 IP 地址 | 端 口 号 | 目的 IP 地址 | 端 口 号 |
|---|---|---|---|
| 10.169.247.64 | 20000 | 61.123.110.251 | 80 |

分析：

【问题 1】

局域网常见拓扑结构分总线型、环型和星型，题中家庭网络中有线部分采用星型拓扑结构。

【问题 2】

家庭无线路由器 WAN 口为局域网出口，LAN 口内接设备。故路由器 R1 和校园网连接的是接口 WAN 口，host1 连接的是接口 LAN 口。

【问题 3】

浏览器地址栏中输入 192.168.1.1 地址，通过用户名和密码认证后登录

家庭无线路由器在其连接的客户机上通过浏览器进行配置，操作方法是在 host1 上启动浏览器，在浏览器地址栏中输入 192.168.1.1，输入用户名和密码，通过认证后登录 R1 的配置界面进行配置。

【问题 4】

主机 host1 在 192.168.1.0/24 网段，网关即路由器地址，故 host1 的 Internet 协议属性参数如下。

IP 地址：192.168.1.2～192.168.1.254 中任选一个

子网掩码：255.255.255.0

默认网关：192.168.1.1

【问题 5】

为了使手机、PAD 等移动设备能接入 Internet 必须获取 IP 地址，若采用自动获取 IP 地址，路由器上需开启 DHCP 功能。从题图中可以看出，SSID 为 FAST_8888。

WPA2-PSK 采用的加密算法为 AES。

【问题 6】

校园网提供的 IP 地址为 WAN 口的地址，从题图中可以看出为 10.169.247.64。

【问题 7】

PC1 访问 Internet 资源 Server1 时，在上行过程中至少应做两次 NAT 变换。第一次为家庭路由器，第二次为学校出口。

路由器 R1 上的 NAT 表如表 4-1 所示，PC1 访问 Internet 时经过 R1 后的报文 IP 地址如表 4-2 所示，则 PC1 的 IP 地址为 192.168.1.5，Server1 的 IP 地址为 61.123.110.251。

**答案：**

【问题 1】

(1)　星型

【问题 2】

(2)　WAN

(3)　LAN

【问题 3】

http://192.168.1.1

【问题 4】

(4)　192.168.1.5

(5)　255.255.255.0

(6)　192.168.1.1

【问题 5】

(7)　DHCP

(8)　FAST_8888

(9)　A

【问题 6】

(10) 10.169.247.64

【问题 7】

(11) 1

(12) 192.168.1.5

(13) 61.123.110.251

**例 2**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2015 年 11 月下午试题一)

【说明】

某单位网络拓扑结构如图 4-4 所示，要求办公楼能与互联网物理隔离，所有汇聚交换机

均采用三层交换机。

【问题 1】(8 分)

请为图 4-4 中空缺处(1)～(8)选择合适设备(限选一次)。

(1)～(8)备选答案：

A．网闸　　B．汇聚交换机　　C．核心交换机

D．AP 控制器　　E．出口路由器　　F．IPv6 路由器

G．防火墙　　H．并发与流量控制器(采用桥接模式)

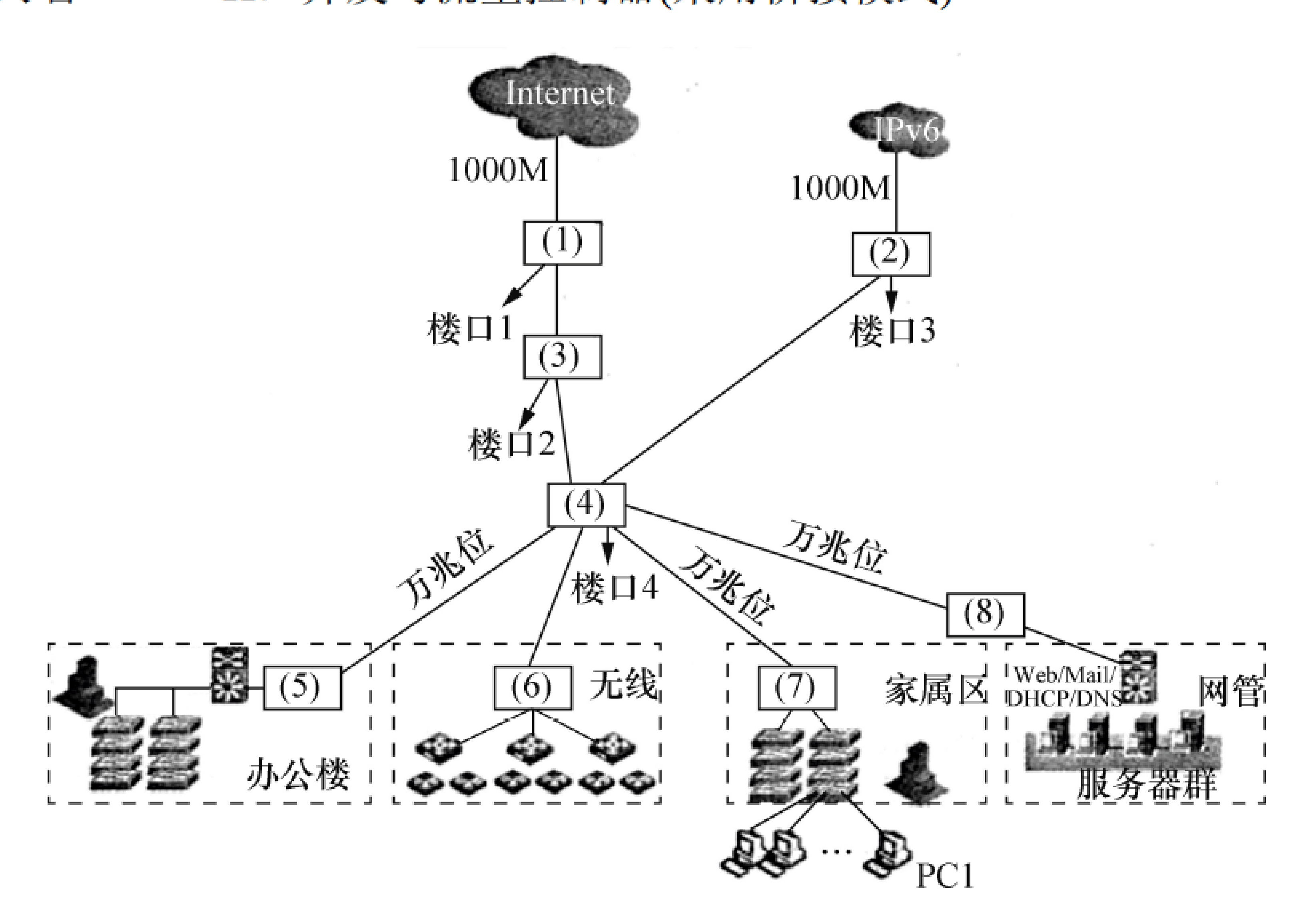



图 4-4　代理服务器功能示意图

【问题 2】(3 分)

在 PC1 中运行 tracert www.aaa.com 命令后，显示结果如图 4-5 所示。

```
C:\Documents and Settings\User>tracert www.aaa.com
Tracing route to www.aaa.com [213.120.116.5]
Over a maximum of 30 hops:

  1    2ms    1ms    <1ms 10.174.255.254
  2    3ms    2ms    1ms 10.155.65.79
  3    <1ms   <1ms   <1ms 10.138.79.1
  4    21     19ms   19ms 123.126.0.218
  5    22ms   23ms   23ms 219.158.16.73
  6    18ms   18ms   18ms 61.150.156.138
  7    19ms   19ms   19ms 213.120.116.5

    Trace complete.
```

图 4-5　命令返回信息

接口 1 的 IP 地址为__(9)__；接口 4 的 IP 地址为__(10)__。

【问题 3】(2 分)

在 PC1 上运 route print 命令后得到 PC1 的路由信息，如图 4-6 所示。

```
C:\Documents and Settings\asus>route print
===========================================================================
Active Routes:
Network Destination    Netmask            Gateway          Interface        Metric
   0.0.0.0             0.0.0.0            10.174.255.254   10.174.107.159     25
  10.174.0.0           255.255.0.0        10.174.107.159   10.174.107.159     25
  10.174.107.159       255.255.255.255    127.0.0.1        127.0.0.1          25
  10.255.255.255       255.255.255.255    10.174.107.159   10.174.107.159     25
  127.0.0.0            255.0.0.0          127.0.0.1        127.0.0.1           1
  224.0.0.0            240.0.0.0          10.174.107.159   10.174.107.159     25
  255.255.255.255      255.255.255.255    10.174.107.159        3              1
  255.255.255.255      255.255.255.255    10.174.107.159   10.174.107.159      1
  Default Gateway:   10.174.255.254
===========================================================================
```

图 4-6　命令返回信息

请完善 PC1 的 Internet 协议属性参数。

IP 地址：__(11)__；

子网掩码：__(12)__；

默认网关：__(13)__。

图 4-6 中第 1 条路由记录的作用是__(14)__。

**分析：**

本题考查简单网络配置与管理知识。

此类题目属常考试题，要求考生认真阅读题目对现实问题的描述，对拓扑、设备、配置等有正确的认识。

**【问题 1】**

本问题考查设备的选择。通常出口处均是路由器，IPv4(图 4-4 中(1)处)与 IPv6(图 4-4 中(2)处)出口处分别是出口路由器和 IPv6 路由器；并发与流量控制器通常放在路由器之后，交换主干之前，故(3)处为并发与流量控制器；(4)处是交换核心，故采用核心交换机；办公楼与互联网物理隔离，故(5)处为网闸；(6)处管理无线局域网接入，故为 AP 控制器；(7)处的汇聚交换机以及(8)处的防火墙较为明显。

**【问题 2】**

接口 1 是经过 3 跳到达的网关，故地址为 10.138.79.1，接口 4 为 10.155.65.79。

**【问题 3】**

由第 3 条记录可以看出，PC1 的 IP 地址为 10.174.107.159，由第 1 条记录可以看出，PC1 的默认网关 IP 地址为 10.174.255.254，子网掩码为 255.255.0.0。第 1 条路由记录的作用是默认路由，即路由列表中无匹配记录时采用的转发路由。

答案：

【问题 1】

(1) E

(2) F

(3) H

(4) C

(5) A

(6) D

(7) B

(8) G

【问题 2】

(9) 10.138.79.1

(10) 10.155.65.79

【问题 3】

(11) 10.174.107.159

(12) 255.255.0.0

(13) 10.174.255.254

(14) 这表示发向任意网段的数据通过本机接口 10.174.107.159 被送往一个默认的网关：10.174.255.254，它的管理距离是 25。

**例 3** 阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2016 年 5 月下午试题一)

【说明】

某网络拓扑结构如图 4-7 所示，路由器 R1 的路由信息如下：

```
C 202.118.1.0/24 is directly connected,FastEthernet0/0
R 202.118.2.0/24[120/1]via 192.168.112.2,00:00:09,Serial0
192.168.112.0/30 is subnetted,1 subnets
C 192.168.112.0 is directly connected,Serial0
```

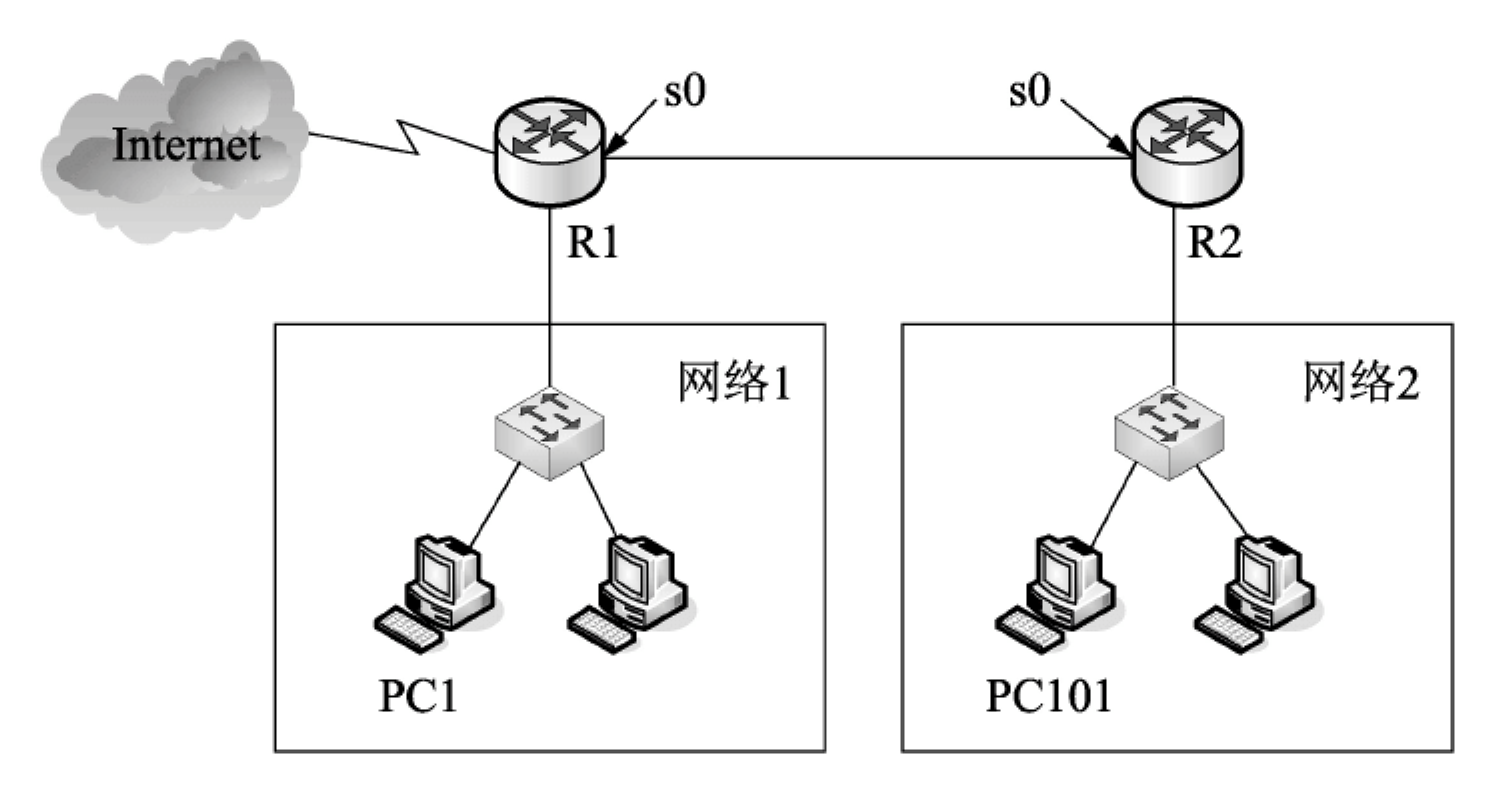



图 4-7 某公司网络拓扑结构

【问题 1】

路由器中查看路由的命令为 Router#__(1)__；

路由器 R1 接口 s0 的 IP 地址为__(2)__；

路由器 R2 接口 s0 的 IP 地址为__(3)__。

【问题 2】

为 PC1 配置 Internet 协议属性参数。

IP 地址：__(4)__；(给出一个有效地址即可)

网掩码：__(5)__。

为 PC101 配置 Internet 协议属性参数。

IP 地址：__(6)__；(给出一个有效地址即可)

子网掩码：__(7)__。

【问题 3】

若 PC1 能 ping 通 PC101，而 PC101 不能 ping 通 PC1，可能原因是__(8)__。

若 PC1 不能 ping 通 PC101，但可以和 PC101 进行 QQ 聊天，可能原因是__(9)__。

(8)、(9)备选答案：

A．PC101 上 TCP/IP 协议安装错误

B．R2 没有声明网络 2

C．R1 没有声明网络 1

D．PC101 上设置了禁止 ICMP 攻击

【问题 4】

填充表 4-3，完成路由器 R2 上网络 2 的用户访问 Internet 的默认路由。

表 4-3　答题表

| 目的网络 IP 地址 | 子网掩码 | 下一跳 IP 地址 | 接口 |
|---|---|---|---|
| (10) | (11) | (12) | (13) |

(10)～(13)备选答案：

A．0.0.0.0

B．255.255.255.255

C．202.118.1.0

D．192.168.112.1 或 R1 的 S0

E．192.168.112.2 或 R2 的 S0

分析：

【问题 1】本问题重点考查路由表查看、IP 地址配置。

(1) 路由器中，查看路由信息，使用命令 show ip route。

(2) 由图 4-7 可知，路由器 R1 的路由信息中网络 202.118.2.0/24 是通过 RIP 路由协议产生，下一跳为 192.168.112.2，故路由器 R1 接口 s0 的 IP 地址为 192.168.112.1；路由器 R2 接口 s0 的 IP 地址为 192.168.122.2。

【问题 2】本问题重点考查主机 IP 地址配置

由路由器路由记录可知，网络 202.118.1.0/24 与路由器 R1 直连，网络 202.118.2.0/24 不直接相连，通过 RIP 协议可达。结合拓扑结构可知，PC1 属于网络 202.118.1.0/24，PC101 属于网络 202.118.2.0/24。

因此，PC1 IP 地址为 202.118.1.1～254，子网掩码为 255.255.255.0，PC101 IP 地址为 202.118.2.1～254，子网掩码为 255.255.255.0。

**【问题 3】**本问题重点考查主机之间通信。

(1) 若 PC1 能 ping 通 PC101，而 PC101 不能 ping 通 PC1。首先若 PC101 上 TCP/IP 协议安装错误，PC1 是不能 ping 通 PC101 的，由此将 A 排除；其次 R1 的路由表上以显示 202.118.2.0/24，故 R2 声明了网络 2，由此将 B 排除；若 PC101 上设置了禁止 ICMP 攻击，PC1 是不能 ping 通 PC101 的，由此排除 D；若 R1 没有声明网络 1，网络 1 与 R1 直连，其能看到网络 1，R2 看不到网络 1，故 PC101 不能 ping 通 PC1，C 正确。

(2) 若 PC1 不能 ping 通 PC101，但是可以和 PC101 进行 QQ 聊天。PC101 上 TCP/IP 协议安装错误、R2 没有声明网络 2，以及 R1 没有声明网络 1 都不成立，只有 PC101 上设置了禁止 ICMP 攻击正确，答案 D。

**【问题 4】**本问题重点考查默认路由。

默认路由是缺省路由，即路由器中已有路由均匹配不上来时采用的路由。目的网络 IP 地址和子网掩码均为 0.0.0.0，路由器 R2 上网络 2 的用户访问 Internet 的默认路由，经过 R2 接口 S0(192.168.112.2)，下一跳为 R1 的接口 S0(192.168.112.1)。

**答案：**

**【问题 1】**

(1) show ip route

(2) 192.168.112.1

(3) 192.168.112.2

**【问题 2】**

(4) 202.118.1.1～254

(5) 255.255.255.0

(6) 202.118.2.1～254

(7) 255.255.255.0

**【问题 3】**(8) C　(9) D

**【问题 4】**

(10) A　(11) A　(12) D　(13) E

**例 4**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2016 年 11 月下午试题一)

**【说明】**

某单位有两间办公室，通过 ADSL 接入 Internet，内网由若干台计算机组成局域网，手机和笔记本计算机均可通过无线方式接入 Internet。为保证无线设备访问 Internet，在房间二安装一个无线路由器。ASDL Modem 和无线路由器的默认管理地址分别是 192.168.1.1 和 192.168.1.25，网络拓扑如图 4-8 所示。

地址分配采用以下两种方法。

方法一：房间一通过 ADSL Modem 为用户分配地址，地址范围为 192.168.10.10～192.168.10.20；房间二通过无线路由器为用户分配地址，地址范围为 192.168.20.10～192.168.20.20。

方法二：两个房间均采用 192.168.10.10～192.168.10.40 地址。

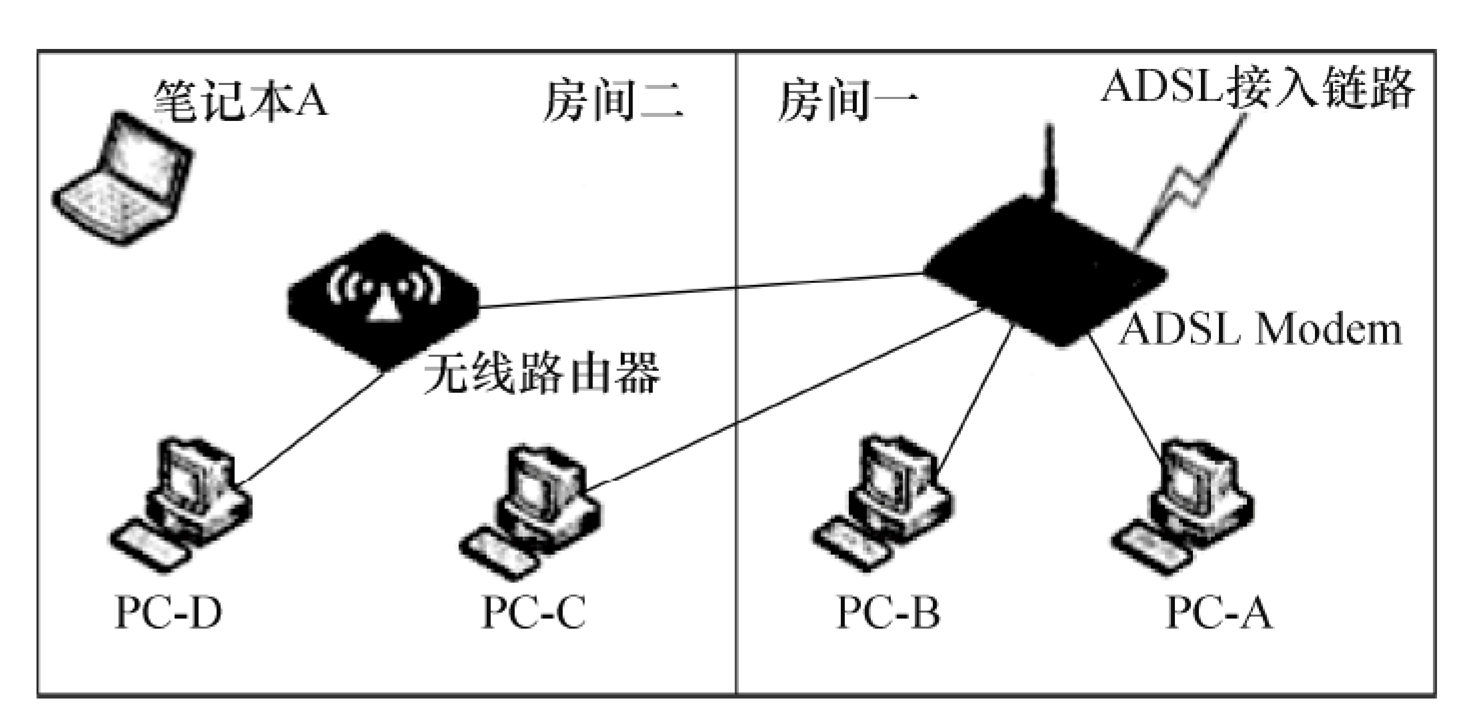



图 4-8　某单位网络拓扑结构

**【问题 1】**

图 4-8 中，ASDL Modem 有 3 个 LAN 口以及 1 个 iTV 口、1 个 DSL 口。ADSL Modem 通过__(1)__接口连接电话线，通过__(2)__接口对 ADSL Modem 进行调试；无线路由通过__(3)__接口与 ADSL Modem 连接。

**【问题 2】**

在图 4-8 中，若采用方法一进行地址分配，PC-D 的地址是__(4)__，网关地址是__(5)__。此时无线路由器的工作模式应设置为__(6)__，其网关地址是__(7)__。

(5)　备选答案：

A．192.168.1.1

B．192.168.1.253

C．192.168.20.253

D．192.168.10.1

(6)　备选答案：

A．接入点模式

B．无线路由模式

C．中继模式

D．桥接模式

(7)　备选答案：

A．192.168.1.1

B．192.168.1.253

C．192.168.20.253

D．192.168.10.1

**【问题 3】**(6 分)

网络在图 4-8 中，若采用方法二进行地址分配，PC-D 设备获取的地址是__(8)__，网关是__(9)__。若无线路由器的工作模式从中继模式变为桥接模式时，无线路由器的 SSID 号及加密

方式 (10) 要与 ADSL Modem 一致。

(9) 备选答案：

A. 192.168.1.1

B. 192.168.1.253

C. 192.168.20.253

D. 192.168.10.1

(10) 备选答案：

A. 一定

B. 不一定

**分析：**

本题考查宽带接入与无线路由器配置的基础知识。要求考生熟悉 ADSL Modem 与无线路由器的接口标识和连线方法，掌握配置此类设备的基本操作要点。

无线路由器的工作模式一般分为路由模式、AP 模式、中继模式、桥接模式和客户端模式。路由模式是无线路由器最常见的模式，通过 DSL 口或 WAN 口接入 Internet。当需要扩大无线信号的覆盖范围时，可以使用中继模式或桥接模式。

**【问题 1】**ADSL Modem 的 LAN 口用于连接网络内部设备，如计算机、交换机或无线路由器等。ADSL Modem 的 iTV 口是电信等 ISP 商为网络用户提供的一种数字电视节目的业务，不能随意进行配置。DSL 口用来接电话线，通过电话线作为传输介质解决发生在网络服务商与最终用户间的“最后一公里”的传输瓶颈。

**【问题 2】**采用方法一对用户地址进行分配，不同房间分配了不同的地址段，根据题中给定的地址段和备选答案，PC-D 获得的地址在 192.168.20.10～192.168.20.20 中任意一个，网关是 192.168.20.253。无线路由器对 PC-D 的地址进行了地址转换，是地址转换无线路由模式与接入点模式的主要区别，因此该题中无线路由器配置的工作模式是无线路由模式。

**【问题 3】**采用方法二对用户地址进行分配，不同房间分配了相同的地址段，根据题中给定的地址段和备选答案，PC-D 获得的地址在 192.168.10.10～192.168.10.40 中任意一个，网关是 192.168.10.1。在无线路由器上进行中继模式和桥接模式的配置，SSID 号和加密方式有所不同，桥接模式下可以自定义不同的 SSID 号和加密方式。

**答案：**

**【问题 1】**(1) DSL　　(2) LAN　　(3) WAN

**【问题 2】**(4) 192.168.20.10～192.168.20.20 中任意一个

(5) C　(6) B　(7) D

**【问题 3】**(8) 192.168.10.10～192.168.10.40 中任意一个

(9) D　(10) B

**例 5**　阅读以下说明，回答问题 1 至问题 3，将解答填入答题纸对应的解答栏内。(2017 年 5 月下午试题一)

**【说明】**

某企业网络拓扑结构如图 4-9 所示，租用 ADSL 宽带实现办公上网，配备一台小型路由器，实现 ADSL 自动拨号和 DHCP 服务功能，所有内部主机(包括台式机和笔记本)通过

路由器实现 Internet 资源的访问。该网络的 IP 地址段为 192.168.1.0/24，网关为 192.168.1.254，防病毒服务器的 IP 地址为 192.168.1.1，网络打印机的 IP 地址为 192.168.1.2，其他 IP 地址均通过 DHCP 分配。

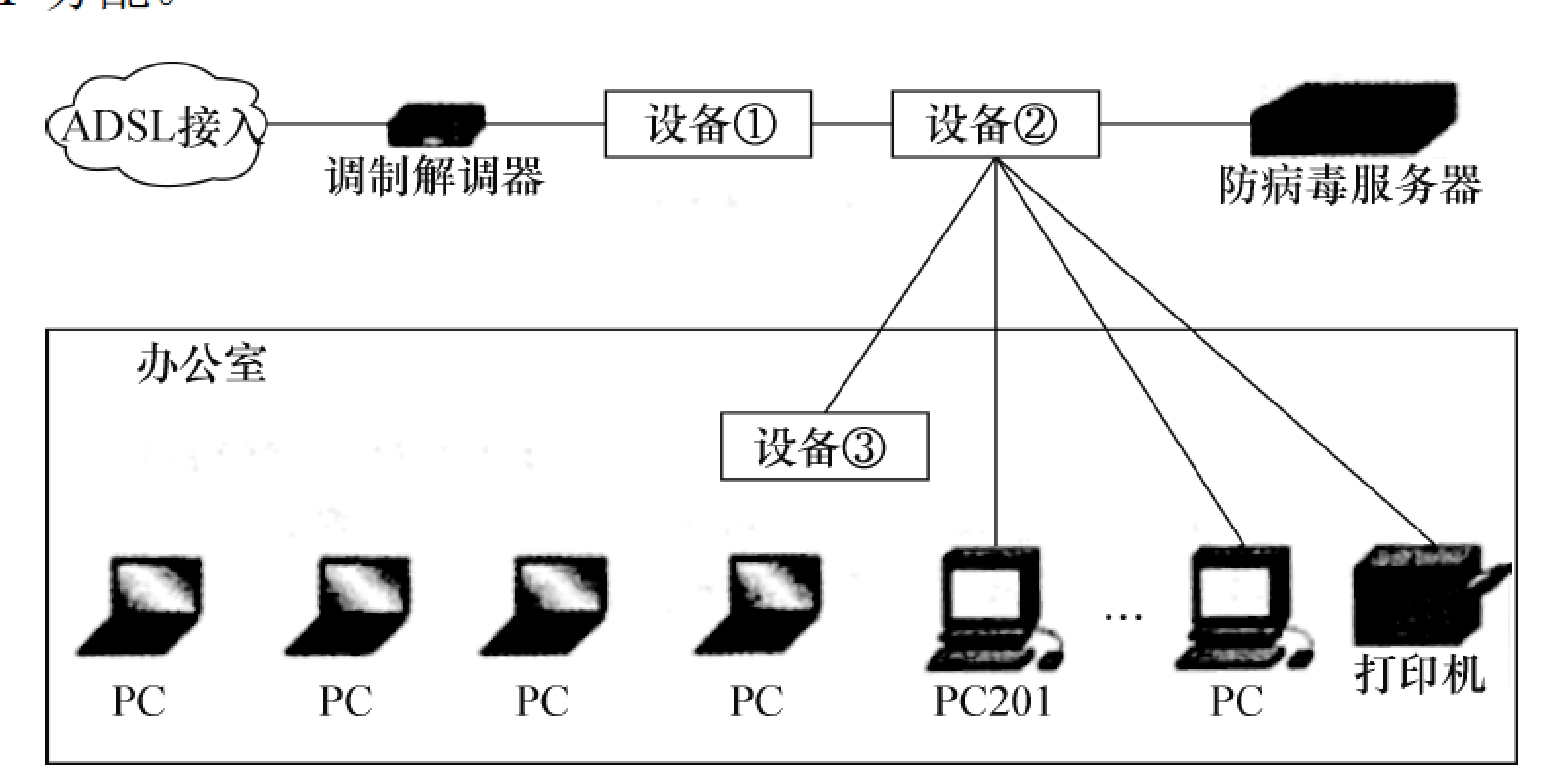



图 4-9　某企业网络拓扑结构

【问题 1】

在图 4-9 中，设备①处应部署__(1)__，设备②处应部署__(2)__，设备③处应部署__(3)__。

(1)～(3)备选答案：

A．交换机　　B．无线 AP　　C．路由器

【问题 2】

图 4-10 所示为路由器的 ADSL 配置页面，WAN 口连接类型应选择__(4)__；图 4-11 所示为路由器的 DHCP 服务页面，地址池开始地址为__(5)__；结束地址为__(6)__；图 4-12 所示为路由器的 LAN 口配置页面，此处的 IP 地址为__(7)__。

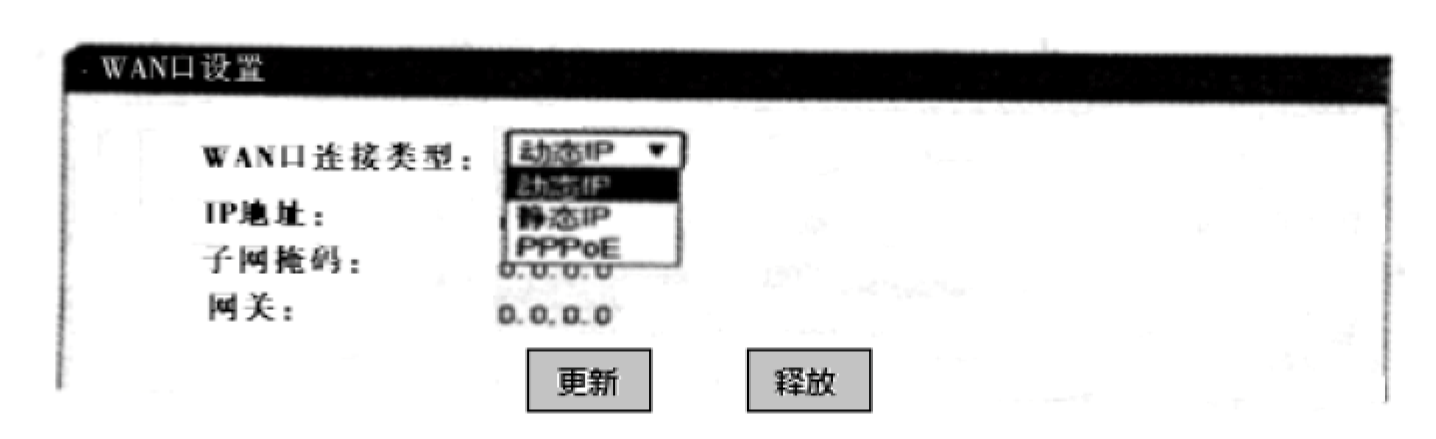



图 4-10　路由器 ADSL 配置页面

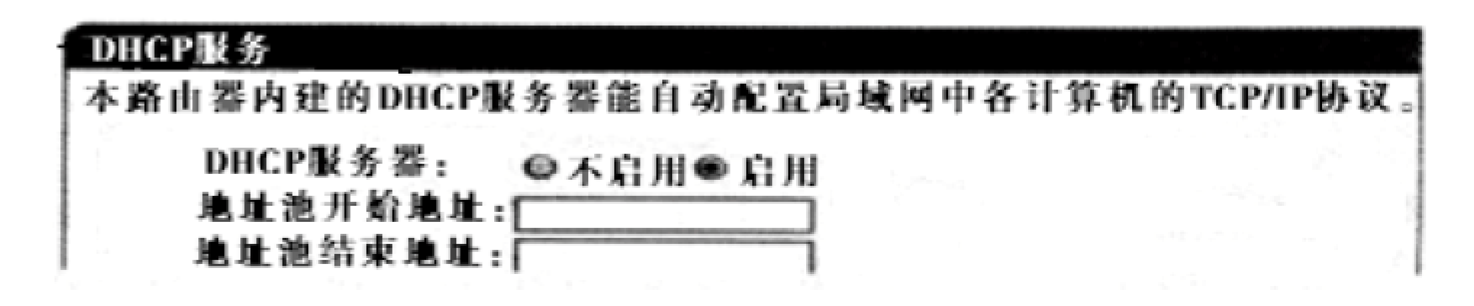



图 4-11　路由器 DHCP 服务页面

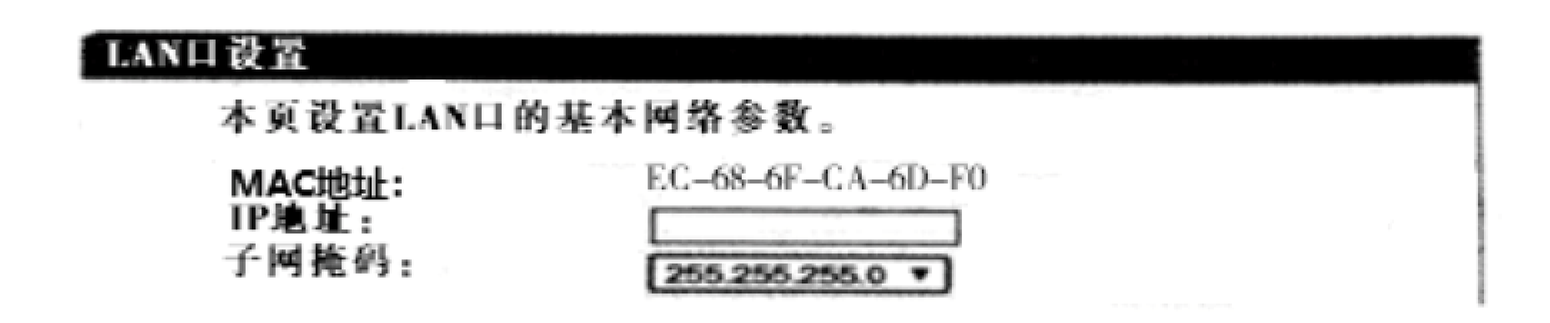



图 4-12　路由器 LAN 口配置页面

【问题 3】

图 4-13 中，PC201 主机发生网络故障，无法访问互联网，网络管理员在该主机 Windows 的命令行窗口输入__(8)__命令，结果如图 4-13 所示，可判断该主机故障为__(9)__。在命令行窗口输入__(10)__命令后该主机恢复正常。

接口：192.168.1.10 ---0xb

| Internet 地址 | 物理地址 | 类型 |
|---|---|---|
| 192.168.1.10 | 00-1b-a9-c4-7d-0c | 动态 |
| 192.168.1.22 | 78-02-f8-f0-fc-c4 | 动态 |
| 192.168.1.254 | 78-02-f8-f0-fc-c4 | 动态 |
| 224.0.0.22 | 01-00-5e-00-00-16 | 静态 |
| 224.0.0.251 | 01-00-5e-00-00-fb | 静态 |
| 224.0.0.252 | 01-00-5e-00-00-fc | 静态 |
| 239.255.255.250 | 01-00-5e-7f-ff-fa | 静态 |

图 4-13　命令返回信息

(8)备选答案：

A．ping　　B．arp　　C．nslookup　　D．tracert

(10)备选答案：

A．arp-s 192.168.1.22 ec-88-8f-ca-8d-fO

B．ping 192.168.1.254

C．arp-s 192.168.1.254 ec-88-8f-ca-8d-fO

D．tracert 192.168.1.254

分析：

【问题 1】

(1) ①处的设备应能为内部网络接入 Internet 提供路由，因此该处为路由器。

(2) ②处的设备负责公司内部所有台式计算机及打印机的 Internet 接入，因此该处为交换机。

(3) ③处的设备负责公司内部笔记本无线接入 Internet，因此该处为无线 AP。

【问题 2】

(4) 因为要实现通过路由器，实现 ADSL 自动拨号和 DHCP 服务功能，所以 WAN 口连接类型应选择 PPPOE。

(5)～(7)因为该网络的 IP 地址段为 192.168.1.0/24，网关为 192.168.1.254，防病毒服务器的 IP 地址为 192.168.1.1，网络打印机的 IP 地址为 192.168.1.2。所以图 4-11 所示的路由器 DHCP 服务页面中地址池开始地址为 192.168.1.3，结束地址为 192.168.1.253。而图 4-12 所示的路由器的 LAN 口配置页面中，此处的 IP 地址为一般和网关地址保持一致，为 192.168.1.254。

【问题 3】

(8) 图 4-13 中显示的为输入 arp 命令后返回的结果。

(9) 因为通过 arp 命令返回的网关 MAC 地址和图 4-12 给的 MAC 不一致，所以判断该

主机发生了 ARP 欺骗。

(10) 在发生了 ARP 欺骗后，可以在命令行窗口输入 arp -s 192.168.1.254 ec-88-8f-ca-8d-f0 命令在 PC 上绑定安全网关的 IP 和 MAC 地址。

**答案：**

**【问题 1】**

(1) C　　(2) A　　(3) B

**【问题 2】**

(4) PPPoE

(5) 192.168.1.3

(6) 192.168.1.253

(7) 192.168.1.254

**【问题 3】**

(8) B

(9) 发生了 ARP 欺骗

(10) C

**例 6**　阅读以下说明，回答问题 1 至问题 6，将解答填入答题纸对应的解答栏内。(2017 年 11 月下午试题一)

**【说明】**

某便利店要为收银台 PC、监控摄像机、客户的无线终端等提供网络接入，组网方案如图 4-14 所示。

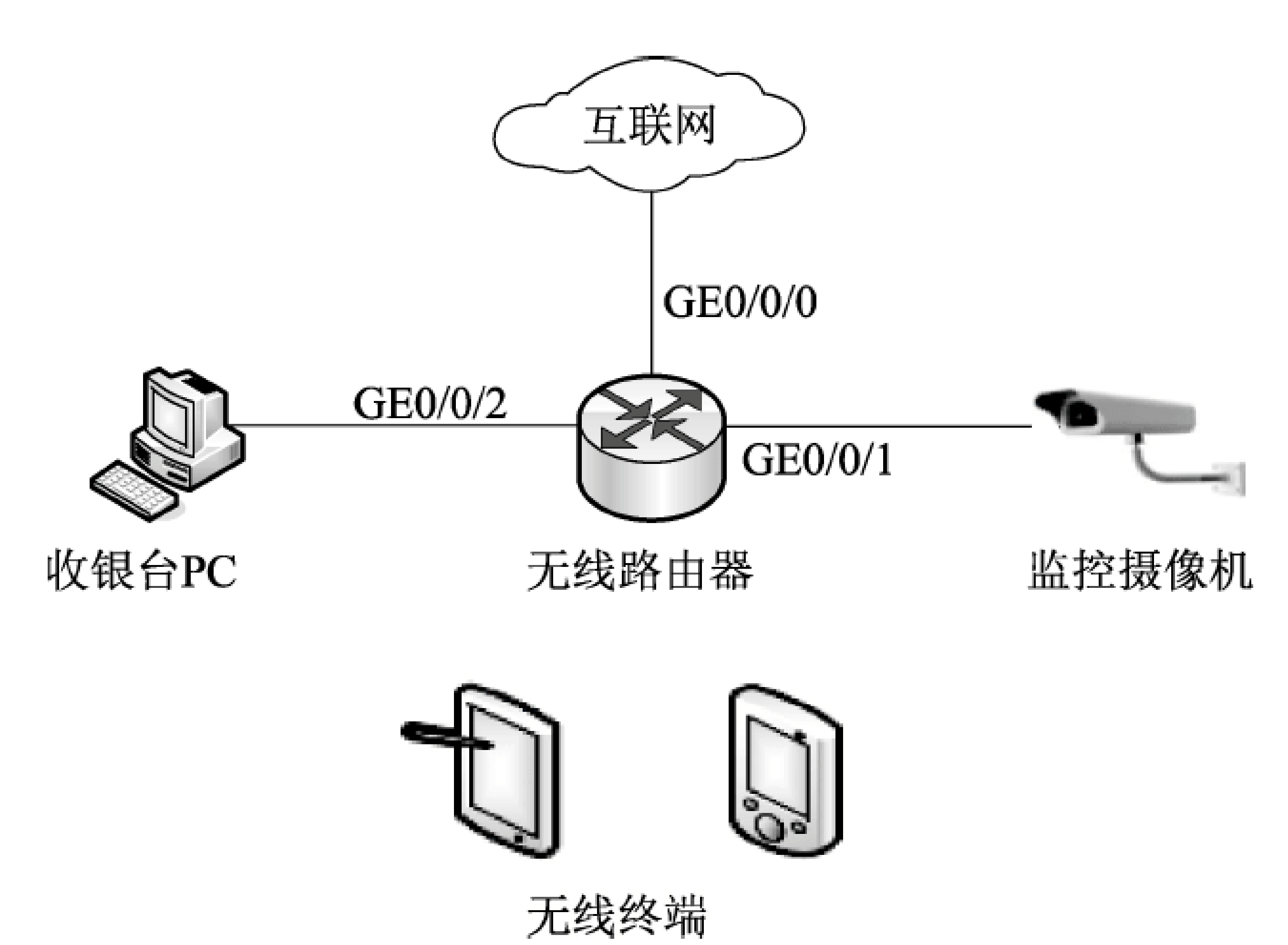



**图 4-14　便利店组网方案**

网络中各设备 IP 分配和所属 VLAN 如表 4-4 所示，其中 VLAN1 的接口地址是 192.168.1.1，VLAN10 的接口地址是 192.168.10.1。

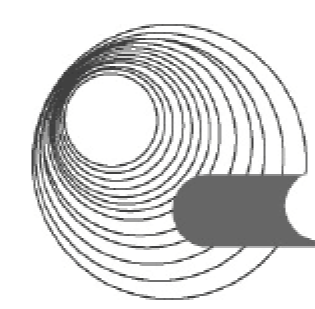




表 4-4　网络设备 IP 分配和所属 VLAN 表

| 项　目 | 数　据 |
|---|---|
| GE0/0/0 地址 | PPPoE 方式获取 33.33.33.33 |
| NAT 方式 | Easy IP |
| 有限网段地址(固定地址) | 192.168.1.0/24;VLAN1 |
| 收银台 PC 地址 | 192.168.1.254/24;VLAN1 |
| 摄像机地址 | 192.168.1.250/24;VLAN1 |
| 无线网断地址(动态分配) | 192.168.10.0/24;VLAN10 |

**【问题 1】**

配置无线路由器，用网线将 PC 的<u>　(1)　</u>端口与无线路由器相连。在 PC 端配置固定 IP 地址为 192.168.l.x/124，在浏览器地址栏输入 http://192.168.1.1，使用默认账号登录<u>　(2)　</u>界面。

(1)备选答案：

A．RJ45　　　B．COM

(2)备选答案：

A．命令行　　　B．Web 管理

**【问题 2】**(4 分)

有线网段配置截图如图 4-15 所示。

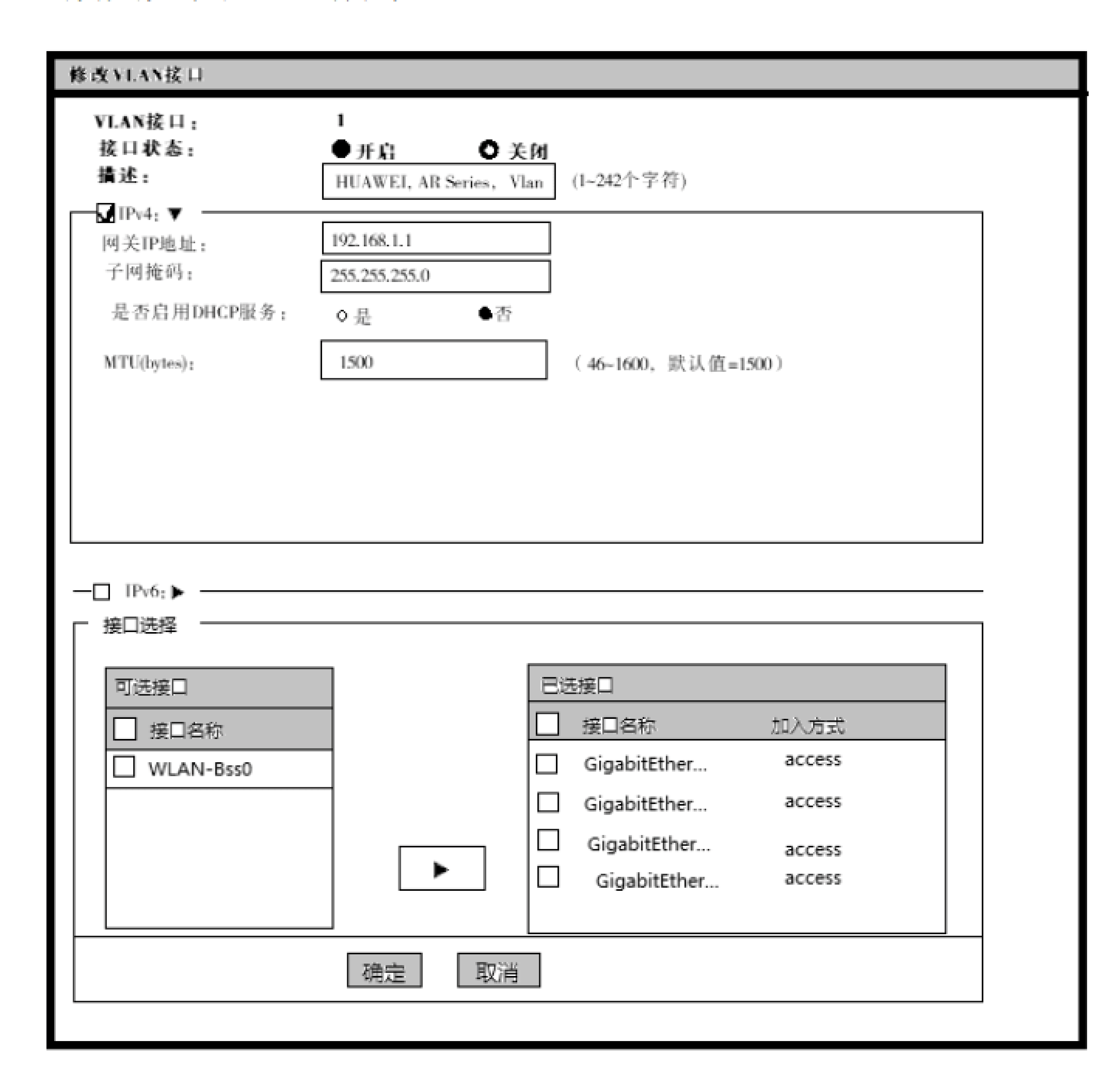



图 4-15　有限网段配置截图

参照表 4-4 和图 4-15，给出无线网段的属性参数。

VLAN 接口(VLAN 编号)：<u>　(3)　</u>；

接口状态：__(4)__；

是否启用 DHCP 服务：__(5)__。

【问题 3】

图 4-15 中参数 MTU 的含义是__(6)__，在__(7)__中 MTU 默认数值 1500B。

(6)备选答案：

A. 最大数据传输单元　　　B. 最大协议数据单元

(7)备选答案：

A. 以太网　　　B. 广域网

【问题 4】(3 分)

某设备得到的 IP 地址是 192.168.10.2 ，该设备是__(8)__。

(8)备选答案：

A. 路由器　　B. 手机　　C. 摄像机　　D. 收银台 PC

【问题 5】(3 分)

图 4-16 是进行网络攻击防范的配置界面。该配置主要是对__(9)__、__(10)__类型的攻击进行防范。




图 4-16　网络攻防配置界面

(9)、(10)备选答案：(不分先后顺序)

A. DOS　　B. DDOS　　C . SQL 注入　　D. 跨站脚本

【问题 6】

该便利店无线上网采用共享密钥认证，采用 WPA2 机制和__(11)__位 AES 加密算法。

(11)备选答案：

A. 64　　B. 128

**分析：**

【问题 1】

配置无线路由器，用网线将 PC 的 RJ-45 端口与无线路由器相连。在 PC 端配置固定 IP 地址为 192.168.1.x/124，在浏览器地址栏输入 http:// 192.168.1.1，使用默认账号登录 Web 管理界面。

【问题 2】

参照表 4-4 和图 4-15，给出无线网段的属性参数。

- VLAN 接口(VLAN 编号)：10。
- 接口状态：开启。
- 是否启用 DHCP 服务：启用。

**【问题 3】**

通信术语最大传输单元(Maximum Transmission Unit，MTU)是指一种通信协议的某一层上面所能通过的最大数据包大小(以字节为单位)。最大传输单元通常与通信接口有关(网络接口卡、串口等)。

因此，图 4-15 中参数 MTU 的含义是最大数据传输单元，在以太网中 MTU 默认数值 1500B。

**【问题 4】**

某设备得到的 IP 地址是 192.168.10.2 ，该设备是手机。192.168.10.2 地址属于动态分配的无线网段地址。

**【问题 5】**

SYN Flood 攻击防范、UDP Flood 攻击防范、ICMP Flood 攻击防范主要是针对 DOS 和 DDoS 类型的攻击的。

**【问题 6】**

AES 的基本要求是，采用对称分组密码体制，密钥长度的最少支持为 128 位。

答案：

**【问题 1】**

(1) A　　(2) B

**【问题 2】**

(3) 10　　(4) 开启　　(5) 启用

**【问题 3】**

(6) A　　(7) A

**【问题 4】**

(8) B

**【问题 5】**

(9)、(10) A、B(顺序无关系)

**【问题 6】**

(11) B

## 4.2.3　同步练习

1. 某公司内部有一个采用 TCP/IP 作为传输协议的 100Base-TX 局域网，包括一台服务器和 20 台客户机，通过一台 16 端口的交换机与一台 8 端口共享集线器级联，其网络结构如图 4-17 所示。服务器上运行 DHCP 服务软件，客户机的 IP 地址由 DHCP 服务程序自动分配。主机 B 登录网络后在网上邻居中只能看到自己的主机名，而看不到服务器和其他客户机的主机名，列出可能出现的硬件、软件故障。

2. 有一小型局域网，服务器为 Windows NT 操作系统，各工作站为 Windows 98 操作系统。以前局域网一直工作正常，后来有一台工作站重新安装 Windows 98 之后，这台计算机通过网上邻居浏览其他计算机的速度非常慢，而且只能看到一部分计算机，有的计算机却

看不到，而其他计算机相互之间一切正常。检查 IP 地址与子网掩码没有错误，域名与工作组也相同。列出可能出现该问题的原因。

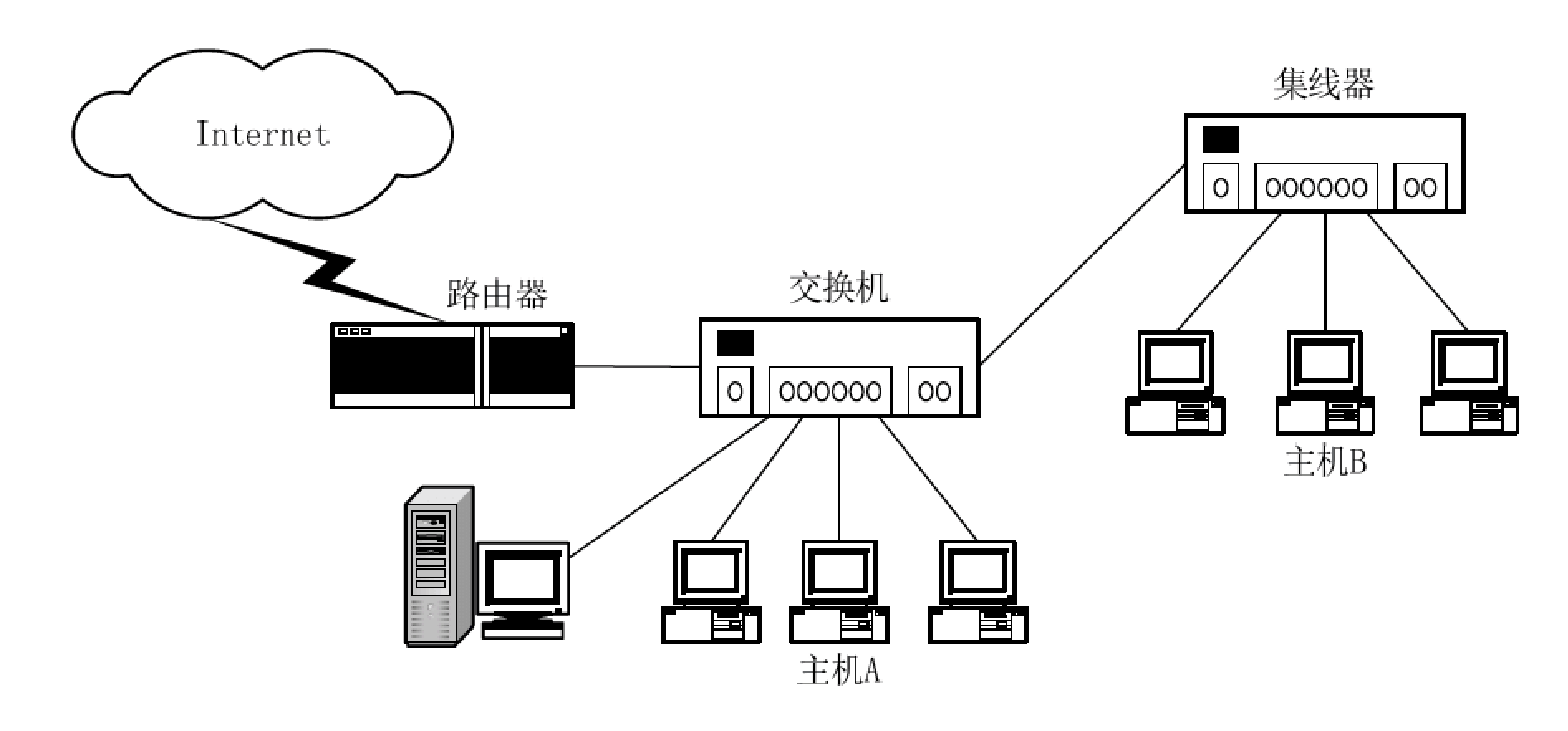



图 4-17　某公司网络结构

3．有一台 PC 无法访问其他计算机和 Internet，通过 ping 命令 ping 127.0.0.1 成功，ping 自己的网卡地址却不成功。请列出可能出现的故障原因。

4．有一台客户机，能够通过网上邻居看到其他客户机和服务器，但就无法访问到 Internet(通过 IP 地址也不行)，但其他客户机却可以。请问最有可能的原因是什么？

5．某公司的域名为 abc.com.cn，内部有一个名字为 www.abc.com.cn 的 Web 服务器，有一台客户机在浏览地址栏中输入 www.abc.com.cn 却无法访问内部的 Web 服务器，输入 Web 服务器的 IP 地址却可以访问，但其他客户机却可以。请问最有可能的原因是什么？

6．网络配置如下：两个子网、一个路由器。路由器有两个接口：网络 A 为 167.191.32.1，网络 B 为 167.191.64.1，所有计算机使用一个子网掩码 255.255.224.0。你的 Windows 2000 工作站连接不到网络 A 上的远程服务器，但网络 B 上所有其他工作站都能连接上。你的工作站位于网络 B。当在工作站上运行 ipconfig/all 命令时，接收到如下输出。

IP 地址是 167.191.82.17；子网掩码是 255.255.224.0；默认网关是 167.191.32.1。导致这一问题的最可能原因是什么？

## 4.2.4　同步练习参考答案

1. 硬件故障主要有网卡故障、通信介质故障(包括网线、跳线或信息插座故障)、Hub 硬件故障(包括 Hub 电源未打开、Hub 硬件故障或 Hub 端口硬件故障)，软件故障包括网卡驱动程序未安装或安装不正确、网络协议未安装或设置不正确、DHCP 服务器设置错误或 IP 地址资源不足。

2. 没有安装 NetBEUI 协议、网卡驱动程序有问题、Windows NT 没有活动目录功能。

3．网卡坏了、IP 地址与其他主机冲突。

4．默认网关没有设置或设置不正确。

5．TCP/IP 属性的 DNS 服务器设置错误或没设置。

6．错误的默认网关，默认网关应当为 167.191.64.1。

## 4.3 本 章 小 结

本章知识点在 2009 年的新大纲中基本没有改变，只是一些表述方式的调整。

这部分主要介绍了常用网络工具的使用；简单网络故障的分析、定位、诊断和排除。

本章内容为下午科目的重点内容，尤其是网络管理命令。本章的每小节中都组织了一些针对水平考试的典型例题分析和同步训练，这些题目基本上涵盖了大纲规定的知识要点。

## 4.4 达标训练题及参考答案

### 4.4.1 达标训练题

1．ping 命令的“-n count”参数的含义是什么？

2．命令“netstat -s -p TCP 60”的含义是什么？

3．有一小型局域网，一台服务器用作 DHCP 服务器，为各客户机分配 IP 地址，有 20 台客户机，它们通过一台 24 口 Hub 相连。有一台 Windows 2000 客户机启动时无法访问 Internet，运行 ipconfig/all 命令后显示 MAC 地址为 00-00-E8-6E-24-2F，IP 地址为 0.0.0.0，子网掩码为 0.0.0.0，DHCP 服务器地址是 255.255.255.255。请列出可能出现的硬件和软件故障。

4．某一公司的域名为 abc.com.cn，内部有一个名字为 www.abc.com.cn 的 Web 服务器，所有客户机在浏览地址栏中输入 www.abc.com.cn 都无法访问内部的 Web 服务器。请问最有可能的问题是什么？

### 4.4.2 参考答案

1．指定要 ping 多少次，具体次数由 count 来指定。

2．每分钟统计一下本机的 TCP 连接情况。

3．硬件故障主要有：网线、跳线或信息插座故障，Hub 电源未打开，Hub 硬件故障或 Hub 端口硬件故障；软件故障主要是 DHCP 服务器设置错误或 IP 地址资源不足，客户机无法租约到 IP 地址。

4．域名服务器工作不正常或配置错误。

# 第 5 章　Web 网站建设

大纲要求：

- Web 网络的规划、建立、管理与维护。
- 使用 HTML 进行网页设计与制作。
- JSP、ASP 动态网页编程技术。
- ADO 的概念和使用。

## 5.1　用 HTML 制作网页

### 5.1.1　考点辅导

#### 5.1.1.1　HTML 简介

超文本标记语言(Hyper Text Mark-up Language，HTML)是 WWW 的描述语言。它是标准通用型标记语言(Standard Generalized Mark-up Language，SGML)的一个应用。

1. HTML 元素

HTML 是标准的 ASCII 文档，其扩展名通常是.html、.htm、.mht、.mhtml 或.shtml，这是常见的 5 种格式。从结构上讲，HTML 由元素组成，它用成对的标签(Tag)，即起始标签和结束标签来组织和定义文档的显示格式。HTML 文件中 HTML 标签的语法格式如下：

<标签名称>标签对象</标签名称>

2. HTML 文档的组成

HTML 文档以<html>标签开始，以</html>标签结束，由文档头和文档体两部分构成。文档头以<head>标签开始，以</head>标签结束；文档体以<body>标签开始，以</body>标签结束。

文档头部分可以包含以下元素。

(1) 窗口标题。它是对 HTML 文档的简单描述，对应标签为<title></title>。

(2) 脚本语言。它是指浏览器解释执行的语句，对应标签为<script></script>。

(3) 样式定义。样式表主要用于格式化网页中的元素，对应标签为<style></style>。

(4) 元数据。它主要提供超文本文档内容和主题的信息，对应标签为<meta>。

文档体包含了可以在浏览器中显示的内容，包含以下元素。

(1) 文本。文本通常以格式化的内容放在文档体中。

(2) 图像。图像主要用于丰富网页的内容。

(3) 链接。链接通常放在文档体中，允许在网站中导航到其他网站。

(4) 多媒体和特定的编程事件。它主要是指包含在 HTML 文档中的 Shockwave、Java Applet 或在线视频等。

3. HTML 文档的结构

HTML 文档的基本结构如下：

```
<html>
<head>
<title> </title>
……
</head>
<body>
……
</body>
</html>
```

#### 5.1.1.2 HTML 常用元素

1. 基本元素

1) 窗口标题(Title)

Title 是 HTML 文档的标题，是对文档内容的概括，在 Web 面浏览时，它出现在浏览器的标题栏。其使用格式如下：

```
<title>窗口标题描述</title>
```

2) 页面标题

页面标题有 6 种，分别为 h1、h2、h3、h4、h5 和 h6，用于表示页面中的各种标题。其使用格式如下：

```
<hn>页面标题描述</hn> (n=1, 2, …, 6)
```

标题可以有对齐属性 align，其属性值有 left(标题居左)、center(标题居中)和 right(标题居右)等。例如：

```
<h2 align="center">居中的二级页面标题</h2>
```

3) 字体

HTML 的字体包括字体大小、字体风格、字体颜色和闪烁等。

字体大小：HTML 有 7 种字号，1 号最小，7 号最大，默认字号为 3。可以用<basefont size=字号>设置默认字号。

字体风格：字体主要包括以黑体<b>、斜体<i>和下画线<u>为代表的物理风格以及特别强调<strong>、源代码<code>和例子<samp>等为代表的逻辑风格。

字体颜色：字体颜色用<font color=#>指定，#可以是 6 位的十六进制数，也可以是 black、navy 和 purple 等英文颜色名称。

闪烁：标签<blink>文本</blink>使文本闪烁，闪烁频率为 1 秒一次。

4) 横线

横线也称水平线，一般用于分隔文本。其 HTML 标签为<hr>，可以指定水平线的对齐、

颜色、阴影和高度等相关属性。例如：

```
<hr  align="center" color=blue  noshade  size="1">
```

表示设定水平线的格式为：居中对齐，蓝色，无阴影，高度为 1。

5)　分行和禁止分行

HTML 标签<br>，表示在此处分行。<nobr>…</nobr>通知浏览器：其中的内容在一行内显示，若一行显示不了，则超出部分被裁剪。

6)　分段

HTML 的分段完全依赖于分段标签<p>段落文本</p>。<p>也可以设定对齐、风格等。例如：

```
<p align="left"  style="color:#FF0000">
```

这表示该段落格式为左对齐，字体颜色为红色。

7)　转义字符与特殊字符

HTML 使用的字符集是 ISO　&859　Larin-1，该字符集中有许多标准键盘上无法输入的字符。对于这些字符只能使用转义字符。常见的需要转义的字符有<、>、&和引号等。

“<”的转义序列为&lt 或&#60；“>”的转义序列为&gt 或&#62；引号的转义序列为&quot 或&#34。例如：

```
<img src="pictures/tower.jpg" alt="安庆府&quot;镇风塔&quot">
```

**注意：** 转义序列各字符间不能有空格；转义字符必须以“;”结束；单独的&不被认为是转义的开始。

8)　背景和文本颜色

窗口背景和文本可以使用以下标签指定：

```
<body background="image-URL"></body>
<body bgcolor="#" text="#" link="# " alink="# " vlink="# "></body>
```

其中，background 表示背景图片；image-URL 表示背景图片的 URL 地址；bgcolor 是指背景颜色，其中#后面是指定的十六进制的红、绿、蓝分量；text 表示文本颜色；link 表示链接颜色；alink 表示活动链接颜色；vlink 表示已访问过的链接颜色。

例如：

```
<body background="images/bg.gif" bgcolor="#FFFFFF" text="#000000"
link="#FF0000" alink="#0000FF" vlink="#FF00FF"></body>
```

表示页面背景图片是 images 文件夹下的 bg.gif 文件，页面背景颜色为白色，文本颜色为黑色，链接颜色为红色，活动链接为蓝色，已访问过的链接为粉红色。

9)　图像

图像(Image)主要用于网页美工。

其使用的基本格式如下：

```
<img src="image-URL" width="#" height="#">
```

其中，image-URL 是图像文件的 URL；width 和 height 表示图像文件的宽度和高度。

另外，可选的图像属性还包括 alt、align 以及 vspace 和 hspace 等。其中，alt 是指图像的替代文字；align 指图像的对齐属性；vspace 和 hspace 表示文本与图像的纵向和横向间距。

例如：

```
<img src="pictures/tower.jpg" width="200" height="100" align="middle" alt=
"镇风塔" vspace="50" hspace="50">
```

10) 列表

列表(List)主要用于列举条目。常用的列表有 3 种格式，即无序列表、有序列表和自定义列表。

(1) 无序列表：以<ul>开始，每一列表条目用<li>引导，黑点表示，最后是</ul>。例如：

```
<ul>
<li>昨天</li>
<li>今天</li>
<li>明天</li>
</ul>
```

(2) 有序列表：以<ol>开始，每一列表条目用<li>引导，数字表示，最后是</ol>。例如：

```
<ol>
<li>昨天</li>
<li>今天</li>
<li>明天</li>
</ol>
```

(3) 自定义列表：以<dl>开始，每一列表条目用<dt>引导，说明用</dd>表示，最后是</dl>。例如：

```
<dl>
<dt>昨天</dt>
<dd>yesterday</dd>
<dt>今天</dt>
<dd>today</dd>
</dl>
```

2. 超文本链接

超文本链接一般由两部分组成：一是被指向的目标；二是指向目标的链接。

1) 统一资源定位器 URL

用于指定访问文档的方法。URL 的构成如下：

```
Protocol://machine.name[:port]/directory/filename
```

其中，Protocol 是指访问该资源所采用的协议，它可以是 HTTP(超文本传输控制协议)、FTP(文件传输控制协议)或 NEWS(网络新闻资源)等；machine.name 是指存放资源的主机 IP；port 是指用于存放资源的主机的相关服务的端口号；directory 和 filename 是该资源的路径和文件名。

例如：

```
http://www.microsoft.com
```

2)　超级链接标签

在 HTML 文档中用链接指向一个目标。其基本格式如下：

```
<a href="URL">字符串</a>
```

例如：

```
<a href="http://www.yahoo.com">雅虎搜索</a>
```

3)　标记

标记也可称为书签或锚记。标识一个链接目标的方法为：

```
<a name="name">text</a>
```

其中，name 属性放置 HTML 文档的全文唯一的标记串，可以用下列方法来指向它：

```
<a href="URL#name">text</a>
```

例如：

```
<a href="http://www.sina.com.cn/sports/news.htm# import">欧洲赛事</a>
```

4)　图像链接

图像也可以建立超级链接。其格式为：

```
<a href="URL "><img src="URL"> </a>
```

例如：

```
<a href="http://www.macromedia.com"><img src="macromedia.gif"></a>
```

5)　图像地图

图像地图可以把图像分成多个区域，每一区域指向不同的目标。图像地图可以分为服务器端和客户端地图。服务器端地图的使用格式为：

```
<a href="/cgi-bin/imagemap/mymap.map">
<img src="mymap.gif" ismap></a>
```

其中，mymap.map 是存放在服务器端/cgi-bin 目录下的图像地图的分区信息文件。

客户端图像地图的使用格式为：

```
<img src="image-URL" usemap="#">
```

其中，image-URL 为用作图像地图的图像；usemap 指客户端地图的标记名。

客户端图像地图的分区信息用<map name=mapname>说明。图像地图的各个区域用<area shape="形状" coords="坐标" href="URL">说明。形状可以是矩形、圆形或多边形。

例如：

```
<img src="map.gif" usemap="#Map">
<map name="Map">
 <area shape="rect" coords="74,100,150,184" href="first.htm">
 <area shape="circle" coords="314,230,65" href="second.htm">
```

```
 <area shape="poly" coords="39,357,166,369,183,313,129,263,49,304"
href="third.htm">
</map>
```

3. 表格

表格(Table)通常用于组织和排列网页信息。表由<table >开始，以</table >结束。表的内容由<thead>、<tbody>、<th>、<tr>和<td>定义。

其基本格式如下：

```
<table>
  <thead>
  <tr>
  <th>… </th>
   ……
  </tr>
  </thead>
  <tbody>
   <tr>
    <td>…</td>
    ……
  </tr>
   ……
  </tbody>
</table>
```

其中，<thead>是表头标签，<tbody>是表格的主体，<th>是列标题标签，<tr>是表中的行标签，<td>是表中的列标签。表 5-1 列出了 table 标签中的一些属性值及其描述。

表 5-1　table 标签中的一些属性值及其描述

| 属　性 | 值 | 描　述 |
|---|---|---|
| align | left, center, right | 规定表格相对周围元素的对齐方式 |
| bgcolor | rgb(*x*,*x*,*x*) | 规定表格的背景颜色 |
| border | pixels | 规定表格边框的宽度 |
| cellpadding | pixels ,% | 规定单元格边沿与其内容之间的空白 |
| cellspacing | pixels, % | 规定单元格之间的空白 |
| width | pixels, % | 规定表格的宽度 |
| height | pixels, % | 规定表格的高度 |

4. 框架

框架(Frame)将浏览器的窗口分成多个区域，每个区域可以单独显示一个 HTML 文档，各个区域的文档可以关联地显示相关内容。

框架的基本结构如下：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
```

```
<title>… </title>
</head>
<frameset >
  <frame src="URL" name="leftFrame">
  <frame src="URL" name="mainFrame">
……
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

框架中可以放置相应的 HTML 页面，主要是通过以下标签来完成的。

1)　<frameset>标签

它是框架集标签，基本参数包括 frameborder、border 和 framespacing 等，主要用于定义整个框架集的行列及边界参数。

2)　<frame>标签

它是单独框架标签，基本参数包括 src 和 name 等，主要用于指定填充该框架的 HTML 文档属性。

3)　<noframe>标签

当浏览器不支持框架时就显示该标签中的内容。

例如：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>上方固定左侧嵌套</title>
</head>
<frameset rows="80,*" cols="*" frameborder="NO" border="0" framespacing="0">
  <frame src="top.htm" name="topFrame" scrolling="NO" noresize>
  <frameset cols="80,*" frameborder="NO" border="0" framespacing="0">
    <frame src="left..htm" name="leftFrame" scrolling="NO" noresize>
    <frame src="main.htm" name="mainFrame">
  </frameset>
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

### 5. 表单

表单(Form)是网页中一种重要的信息收集和交流工具，它在 Web 数据库技术中起着关键性作用。下面是一个包含简单表单对象的 HTML 文本的示例。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>百度搜索</title>
</head>
<body>
<FORM name=f action=http://www.baidu.com/baidu  method="post">
<INPUT class=ff maxLength=100 size=35 name=w>
  <INPUT type=submit value=百度搜索>
</FORM>
</body>
</html>
```

1) 表单标签

标签<FORM>提供表单的功能，由开始标签和结束标签(<FORM>…和</FORM>)组成，表单中可以设置文本框、按钮或下拉菜单等表单域元素。在开始标签中带有两个重要属性，即 ACTION 和 METHOD，分别指定了表单的动作和方法。

2) 文本框

文本框可以分为单行文本框和多行文本框。单行文本框的 HTML 基本标签是：<input type="text" name="textfield">；多行文本框的 HTML 基本标签是：<textarea name="textfield"></textarea>。

3) 按钮

按钮可以分为单选按钮、复选框以及提交、重置按钮。单选按钮的 HTML 基本标签是：<input type="radio" name="radiobutton" value="radiobutton">；复选框的 HTML 基本标签是：<input type="checkbox" name="checkbox" value="checkbox">；提交、重置按钮的 HTML 基本标签分别是：<input type="submit" name="Submit" value="提交">和<input type="reset" name="Submit" value="重置">。

4) 下拉菜单

下拉菜单通过标签<select>实现，其 HTML 基本标签是：<select name="select" size="1"></select>。

表 5-2 列出了表单常用的控件、常用属性及属性值。

**表 5-2　表单常用的控件、常用属性及属性值**

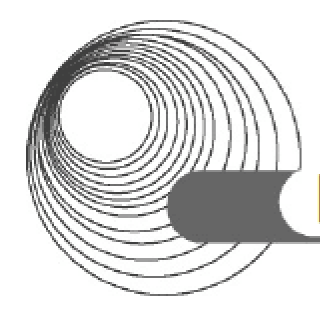
| 控 件 名 | 主要属性 | 属 性 值 |
|---|---|---|
| 文本框 | name | 任意 |
| | type | text |
| | value | 任意(表单实际的值) |
| | size | 数字(文本框的长度) |
| | maxlength | 数字(文本框的最大长度) |

续表

| 控 件 名 | 主要属性 | 属 性 值 |
| --- | --- | --- |
| 文本域 | name | 任意 |
| | type | textarea |
| | cols | 数字(文本域列数) |
| | rows | 数字(文本域行数) |
| 单选按钮 | name | 任意 |
| | type | radio |
| | value | 任意(表单实际的值) |
| | checked | checked(表示单选按钮默认选中) |
| 复选框 | name | 任意 |
| | type | checkbook |
| | value | 任意(表单实际的值) |
| | checked | checked(表示复选框默认选中) |
| 下拉列表框 | name | 任意 |
| | type | select |
| | size | 数字(下拉列表框高度) |
| 下拉列表选项 | type | option |
| | vlaue | 任意(表单实际的值) |
| | selected | selected(该选项默认被选中) |
| 密码 | name | 任意 |
| | type | password |
| | value | 任意(表单实际的值) |
| 提交按钮 | name | 任意 |
| | type | sumbit |
| | value | 任意(按钮实际的值) |
| 重置按钮 | name | 任意 |
| | type | reset |
| | value | 任意(按钮实际的值) |
| 文件框 | name | 任意 |
| | type | file |
| 图像 | name | 任意 |
| | type | image |
| | src | URL(图片路径) |

### 5.1.1.3　应用实例

以下是著名的 Google 搜索引擎首页的 HTML 源文件(注：为了方便读者阅读，作者进行了重新排版)。





```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>Google</TITLE>
<META http-equiv=content-type content="text/html; charset=UTF-8">
<STYLE>
  BODY {FONT-FAMILY: arial,sans-serif}
  TD {FONT-FAMILY: arial,sans-serif }
  A {FONT-FAMILY: arial,sans-serif }
  P {FONT-FAMILY: arial,sans-serif }
 .h {FONT-FAMILY: arial,sans-serif}
 .h {FONT-SIZE: 20px}
 .q {COLOR: #0000cc}
</STYLE>
<SCRIPT>
<!--
  function sf(){document.f.q.focus();}
  function clk(el,ct,cd,sg)
  {  if(document.images)
    {  (new Image()).src="/url?sa=T&ct="+escape(ct)+
         "&cd="+escape(cd)+"&url="+escape(el.href).replace(/\+/g,"%2B")+
         "&ei=WXG6Qs3eO6qmOMPehZwP"+sg;}
        return true;}
  function rbi(f)
  {  if (navigator.appName == "Netscape")
     {  f.biw.value=self.innerWidth;}
      else {  f.biw.value=document.body.clientWidth;}}// -->
</SCRIPT>
<META content="MSHTML 6.00.2900.2135" name=GENERATOR></HEAD>
<BODY text=#000000 vLink=#551a8b aLink=#ff0000 link=#0000cc bgColor=#ffffff
topMargin=3 onload=sf() marginheight="3">
<CENTER>
  <IMG height=110 alt=Google src="logo.gif" width=286>
  <FORM name=f onsubmit=rbi(this); action=/search>
<SCRIPT><!--
 function qs(el)
 {  if (window.RegExp && window.encodeURIComponent)
    { var ue=el.href;var qe=encodeURIComponent(document.f.q.value);
      if(ue.indexOf("q=")!=-1)
      {  el.href=ue.replace(new RegExp("q=[^&$]*"),"q="+qe);}
      else{el.href=ue+"&q="+qe;}
    }
    return 1;}
// -->
</SCRIPT>
<TABLE cellSpacing=0 cellPadding=4 border=0>
  <TBODY>
  <TR>
    <TD noWrap><FONT size=-1><B>网页</B>    
<A class=q id=1a  onclick="return qs(this);"
     href="http://www.google.com/imghp?hl=zh-CN&amp;tab=wi">图片</A>
<A class=q id=2a onclick="return qs(this);"
```

```
    href="http://www.google.com/nwshp?hl=zh-CN&amp;tab=wn">新闻</A>
<A class=q id=3a onclick="return qs(this);"
    href="http://www.google.com/grphp?hl=zh-CN&amp;tab=wg">论坛</A>
<A class=q id=4a onclick="return qs(this);"
  href="http://www.google.com/dirhp?hl=zh-CN&amp;tab=wd">网页目录</A><B>
      <A  class=q  href="http://www.google.com/intl/zh-CN/options/">更多
 »</A></B>
      </FONT></TD></TR></TBODY></TABLE>
<TABLE cellSpacing=0 cellPadding=0>
  <TBODY>
  <TR>
    <TD width="25%"> </TD>
    <TD align=middle>
      <INPUT type=hidden name=biw>
      <INPUT type=hidden  value=zh-CN name=hl>
     <INPUT maxLength=256 size=55 name=q><BR>
     <INPUT type=submit value="Google 搜索" name=btnG>
      <INPUT type=submit value=手气不错 name=btnI></TD>
    <TD vAlign=top noWrap width="25%"><FONT size=-1>  
<A href="http://www.google.com/advanced_search?hl=zh-CN">高级搜索</A><BR>
<A href="http://www.google.com/preferences?hl=zh-CN">使用偏好</A><BR>
<A href="http://www.google.com/language_tools?hl=zh-CN">语言工具</A>
</FONT></TD></TR>
  <TR>
    <TD align=middle colSpan=3><FONT size=-1>
      <INPUT id=all type=radio CHECKED value="" name=lr>
      <LABEL for=all>搜索所有网页</LABEL>
      <INPUT id=ch type=radio value=lang_zh-CN|lang_zh-TW name=lr>
      <LABEL for=ch>搜索所有中文网页</LABEL>
      <INPUT id=il type=radio value=lang_zh-CN name=lr>
      <LABEL for=il>搜索简体中文网页</LABEL>
   </FONT></TD></TR></TBODY></TABLE></FORM>
  <p><FONT size=-1><p></FONT <BR>
  <p><BR><BR><FONT size=-1>
  <A href="http://www.google.com/intl/zh-CN/ads/">广告计划</A> -
  <A href="http://www.google.com/intl/zh-CN/about.html">Google 大全</A> -
  <A href="http://www.google.com/ncr">Google.com in English</A>
  <SPAN id=hp style="BEHAVIOR: url(#default#homepage)"></SPAN>
<SCRIPT>
//<!--
    if (!hp.isHomePage('http://www.google.com/'))
     { document.write("<p><a href=\"/mgyhp.html\"
       onClick=\"style.behavior='url(#default#homepage)';
   setHomePage('http://www.google.com/');\">将 Google 设为首页！</a>");}
//-->
</SCRIPT>
 </FONT>
<P><FONT size=-1>©2005 Google - 搜索 8,058,044,651 张网页</FONT></P>
</CENTER></BODY></HTML>
```

该文档在 IE 浏览器中的运行结果如图 5-1 所示。

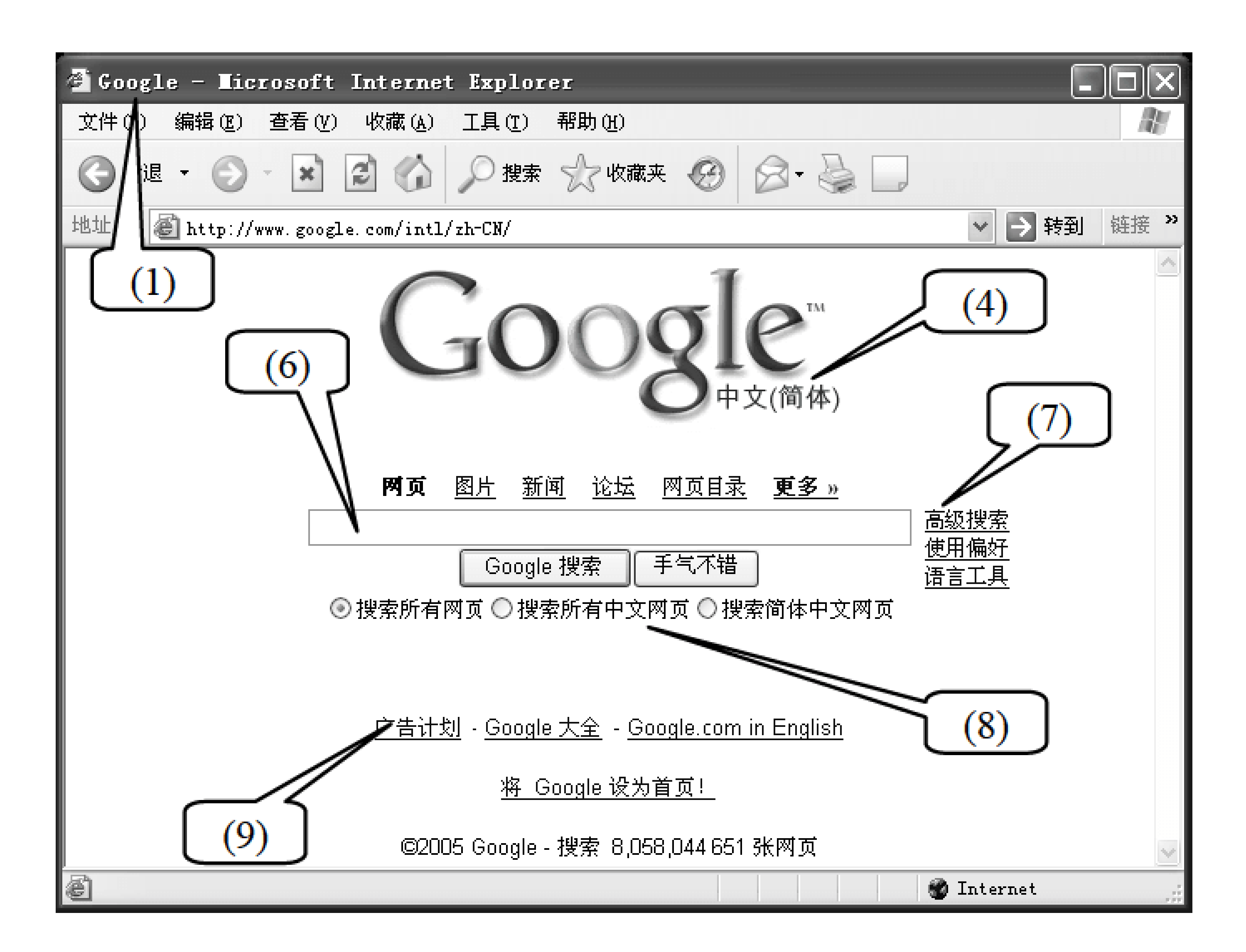



图 5-1 Google 首页

相关 HTML 代码说明如下。

(1) <TITLE>Google</TITLE>，<TITLE>定义网页的标题是 Google。

(2) <STYLE>BODY {FONT-FAMILY: arial,sans-serif}…</STYLE>，<STYLE>定义了网页元素的样式。

(3) <SCRIPT><!--function sf(){…}…// --></SCRIPT>，<SCRIPT>定义了网页使用的 Java Script 函数。

(4) <IMG height=110 alt=Google src="Google.files/logo.gif" width=286>，<IMG>定义了网页中所使用的 LOGO 图片。

(5) <TABLE cellSpacing=0 cellPadding=4 border=0>…</TABLE>，<TABLE>定义了以表格方式排列的网页数据。

(6) <FORM name=f action=/search>…</FORM>，<FORM>定义了网页中的一个表单对象。

(7) <INPUT type=hidden value=zh-CN name=hl>，<INPUT>定义了一个隐含域类型的网页输入数据。

(8) <LABEL for=ch>搜索所有中文网页</LABEL>，<LABEL>定义了表单中的标签对象。

(9) <A href="http://www.google.com/intl/zh-CN/ads/">广告计划</A>，<A>定义了网页中的一个超级链接地址。

## 5.1.2 典型例题分析

**例 1** 阅读下列 HTML 文本和说明，在该 HTML 文本中存在 5 处错误，请指出错误所在的行号、错误原因以及改正的方法，把解答填入答案的对应栏内。

【说明】

这是一个简单的 HTML 文本，显示作者个人主页的登录界面。

HTML 文本如下：

```
(1) <HTML>
(2) <BODY>
(3) <HEAD>
(4) <META NAME="Author" CONTENT="Brent Heslop, David Holzgang">
(5) </HEAD>
(6) <TITLE TITLE="Authors Home Page">
(7) <!-- MAKE SURE BKGND COLOR IS WHITE -->
(8) <BGCOLOR="white">
(9) <IMG ALT="log.jpg" SRC="Welcome to Authors Home page">
(10) <H2><A HREF="http://WWW.authors.public.com">Authors Home Page </A></H2>
(11) <P>Welcome to the authors Web Site. </P>
(12) </BODY>
(13) </HTML>
```

**分析：**本题主要考核 HTML 语言的基本概念和元素。

HTML 文档以<HTML>标签开始，以</HTML>标签结束，由文档头和文档体两部分构成。文档头由<HEAD>开始，</HEAD>结束；文档体由<BODY>开始，</BODY>结束。

HTML 元素主要包括基本标签、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题仅仅涉及了部分基本标签和图像等元素。

**答案：**

① 第(2)行不正确：<BODY>标签的位置不正确。<BODY>和</BODY>作为文档体标签，应该置于<HEAD>和</HEAD>之后。

② 第(6)行不正确：<TITLE>标签的使用不正确。<TITLE >和</TITLE >用于定义网页的标题，两个标签之间为标题的内容；并且<TITLE >和</TITLE >标签应位于<HEAD >和</ HEAD >标签之间。

③ 第(8)行不正确：<BGCOLOR="white">使用不正确。网页背景是通过<BODY>标签的 BGCOLOR 属性指定，如< BODY BGCOLOR="white">。

④ 第(9)行不正确：<IMG ALT="log.jpg" SRC="Welcome to Authors Home page">使用不正确。<IMG>标签的 ALT 属性是指替代文本，SRC 属性是指图片源文件，因此 ALT 属性值和 SRC 属性值应该对调。

⑤ 第(10)行不正确：<H2> 二级标题标签和<A>超级链接标签的顺序不正确，应该调整为<A HREF="http://WWW.authors.public.com"><H2>Authors Home Page </H2></A>。

**例 2** 阅读下列说明和 HTML 文本。在 HTML 文本中存在 5 处错误，请指出错误之处并给出改正的方法。

【说明】

这是一个简单的 HTML 文本，描述了框架的 HTML 语法，显示效果如图 5-2 所示。

HTML 文本如下：

```
(1)<html>
(2)<head>
(3)<title>框架测试</title>
(4)</head>
(5)<meta name="GENERATOR" content="Microsoft FrontPage 4.0">
(6)<frameset rows="64, *">
(7)<frame name="banner"scrolling="no"target="contents"src="header.htm">
(8)<frame name="contents" target="list" src="list.htm">
(9)<frameset cols="150, *">
(10)<frame name="main" src="context.htm">
(11)</frameset>
(12)</frameset>
(13)<noframes>
(14)<body><p>此网页使用了框架。</body>
(15)</noframes>
(16)</html>
```

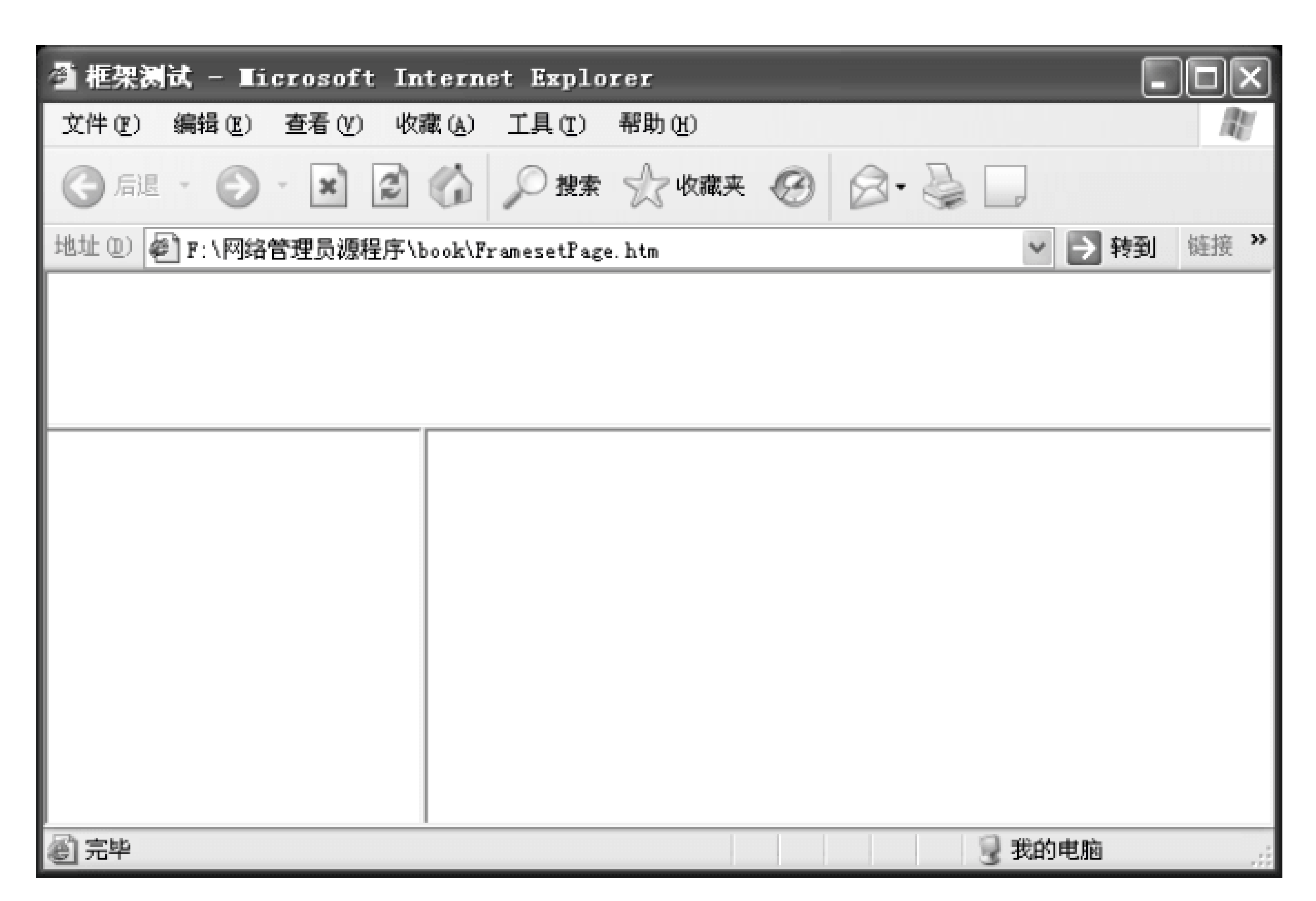



图 5-2　HTML 框架效果

**分析：**本题主要考查考生对 HTML 文档和框架网页结构的掌握情况。<frameset>标签是一个框架容器，它可以将窗口分成若干个框架，框架的 HTML 标签是<frame>。<frame>的个数是由<frameset>标签中的参数决定的。<frameset>标签中还可能包含一个可选的<noframes>标签，其作用是当浏览器不支持或禁用<frame>时，<noframes>标签将提供替代的浏览内容。

**答案：**

① 第(5)行位置不正确：<meta>标签必须位于<head>与</head>标签之间。

② 第(8)行不正确：在<frame>的 target 属性中指定的框架“list”在文本中没有定义，可以改为 banner、contents 或 main 之中的任何一个。

③ 第(9)行位置不正确：根据图像分析，框架结构应该为上左右型，而本例为左右下型，应将第(8)、(9)行互调。

④ 第(13)、(14)、(15)行位置不正确：<noframes>与</noframes>应位于<frameset>与</frameset>之间。

⑤ 第(14)行不正确：<p>与</p>应该成对出现，在文字与</body>之间应添加</p>。

## 5.1.3 同步练习

阅读下面 HTML 文本和说明，在 HTML 文本中存在 5 处错误，请指出这些错误并给出改正的方法。

**【说明】**

这是一个简单的 HTML 文档，显示的是一个网页列表信息，显示界面如图 5-3 所示。

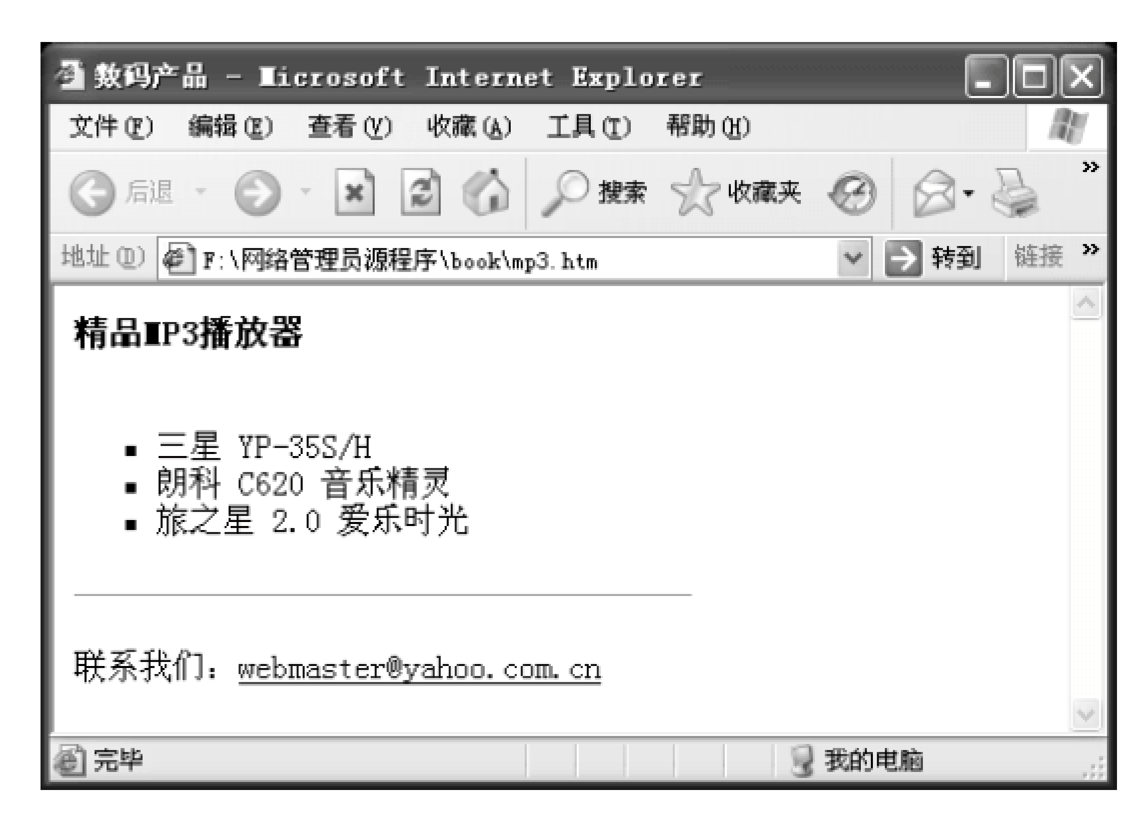



图 5-3 网页列表

HTML 文本如下：

```
(1)<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
(2)"http://www.w3.org/TR/html4/loose.dtd">
(3)<html>
(4)<head>
(5)<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
(6) </head>
(7) <title>数码产品</title>
(8)<body>
(9)<p><strong>精品 MP3 播放器</p></strong>
(10)  <ul type="square">
(11)  <li>三星 YP-35S/H</li>
(12)    <li>朗科 C620 音乐精灵</li>
(13)  </ul>
(14)    <li>旅之星 2.0 爱乐时光</li>
(15) <hr align="left" width="300" size="1">
(16)<p>联系我们:
(17)<a href="mailto:webmaster@yahoo.com"> </a> webmaster@yahoo.com.cn </p>
(18) </html>
(19) </body>
```

### 5.1.4 同步练习参考答案

① 第(7)行不正确：<title>标签必须位于<head>与</head>标签之间。
② 第(9)行不正确：</strong>标签必须位于<p>与</p>之间。
③ 第(13)、(14)行位置不正确：根据图像分析，应将第(13)、(14)行互换。
④ 第(17)行不正确：</p>之前的 webmaster@yahoo.com.cn 应置于</a>之前。
⑤ 第(18)、(19)行位置不正确：根据图像分析，应将第(18)、(19)行互换。

## 5.2 动态网页制作

### 5.2.1 考点辅导

动态网页技术主要依赖于服务器端编辑，包括 CGI 版本、Server-API 程序(NSAPI 和 ISAPI)、JavaServerlets 以及服务器脚本语言。

服务器脚本环境有许多，其中最流行的几种包括 ASP(Active Server Pages)、ASP.NET(基于.NET 架构的 ASP)、JSP(Java Server Pages)、PHP 等。

#### 5.2.1.1 ASP

1. ASP 简介

1) ASP 概述

ASP 是 Active Server Pages(动态服务器页面)的缩写，ASP 可以混合使用 HTML、脚本语言以及组件来创建服务器端功能强大的 Internet 应用程序。ASP 使用 Microsoft 的 ActiveX 技术，它采用封装程序调用对象的技术，从而简化了编程并且加强程序间的协作。

2) ASP 的特点

ASP 运行在服务器端时不需要编译，可在服务器端直接执行，与浏览器无关。ASP 返回标准的 HTML 页面，浏览者查看页面源文件时，看到的是 ASP 生成的 HTML 代码，而不是 ASP 程序代码。

3) ASP 的编程环境

ASP 的编程语言可以是 VBScript 和 JavaScript，而 VBScript 则是系统默认的脚本语言。ASP 的编程语言可以使用普通的文本编辑器进行设计，ASP 程序则以扩展名.asp 的纯文本形式保存在 Web 服务器上的具有可执行权限的虚拟目录之下，供用户通过 WWW 的方式访问。

2. ASP 内嵌对象

ASP 提供了可以在脚本中使用的各种内嵌对象。这些内嵌对象主要用于收集浏览器请求信息、响应浏览器和存储用户的各种信息，从而简化编程工作。ASP 结构提供 6 个内建对象，包括 Request、Response、Application、Session、Server 和 ObjectContext。内建对象

的特殊性在于，它们在 ASP 页内生成且在脚本中使用它们前无须创建。

1)　Request 对象

Request 对象在 HTTP 请求期间，检索客户端浏览器传递给服务器的值。

其使用语法为：

```
Request[.collection|property|method](variable)
```

Request 对象唯一的属性及说明如表 5-3 所示。它提供关于用户请求的字节数量的信息，很少用于 ASP 页，用户通常关注指定值而不是整个请求字符串。

表 5-3　Request 对象的属性及说明

| 属　性 | 说　明 |
|---|---|
| Total Bytes | 只读。返回由客户端发出的请求的整个字节数量 |

2)　Response 对象

Response 对象用来访问服务器端所创建的并发回客户端的响应信息。

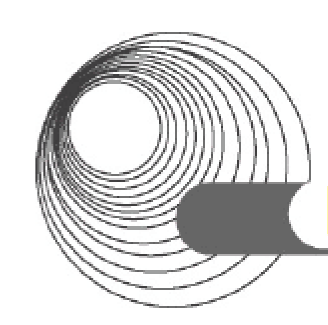
其使用语法为：

```
Response.collection|property|method
```

Response 对象也提供一系列的属性，可以读取和修改，使响应能够适应请求。这些由服务器设置，用户不需要设置它们。需要注意的是，当设置某些属性时，使用的语法可能与通常所使用的有一定差异。这些属性如表 5-4 所示。

表 5-4　Response 对象的属性及说明

| 属　性 | 说　明 |
|---|---|
| Buffer-True\|False | 读写。布尔型。表明由一个 ASP 页所创建的输出是否一直存放在 IIS 缓冲区，直到当前页面的所有服务器脚本处理完毕或 Flush、End 方法被调用。在任何输出(包括 HTTP 报头信息)送往 IIS 之前，这个属性必须设置。因此在 ASP 文件中，这个设置应该在<%@ LANGUAGE=...%>语句后面的第一行 |
| CacheControl "setting" | 读/写。字符型。设置这个属性为“Public”，允许代理服务器缓存页面，如为"Private"，则禁止代理服务器缓存的发生 |
| Charset="value" | 读/写。字符型。在由服务器为每个响应创建的 HTTP Content-Type 报头中附上所用的字符集名称 |
| Content Type ="MIME-type" | 读/写。字符型。指明响应的 HTTP 内容类型，标准的 MIME 类型(如 text/xml 或者 Image/gif)。假如省略，表示使用 MIME 类型 text/lhtml，内容类型告诉浏览器所期望内容的类 |
| Expires minutes | 读/写。数值型。指明页面有效的以分钟计算的时间长度，假如用户请求其有效期满之前的相同页面，将直接读取显示缓冲中的内容，这个有效期过后，页面将不再保留于私有(用户)或公用(代理服务器)缓冲中 |





续表

| 属　性 | 说　明 |
|---|---|
| Expires Absolute#date[time]# | 读/写。日期/时间型。指明当一个页面过期和不再有效时的绝对日期和时间 |
| Is Client Connected | 只读。布尔型。返回客户是否仍然连接和下载页面的状态标志。在当前的页面已执行完毕之前，假如一个客户转移到另一个页面，这个标志可用来中止处理 |
| PICS ("PICS-Label-stringy") | 只写。字符型。创建一个 PICS 报头并将之加到响应中的 HTTP 报头中，PICS 报头定义页面内容中的词汇等级，如暴力、性、不良语言等 |
| Status="Code message" | 读/写。字符型。指明发回客户的响应的 HTTP 报头中表明错误或页面处理是否成功的状态值和信息，如"200 OK"和"404 Not Found" |

3)　Application 对象

可以使用 Application 对象在给定的应用程序的所有用户之间共享信息。基于 ASP 的应用程序与所有的.asp 文件一样在一个虚拟目录及其子目录中定义。因为多个用户可以共享 Application 对象，所以必须由 Lock 和 Unlock 方法以确保多个用户无法同时更改某一属性。

其使用语法为：

```
Application.method
```

Application 对象提供了在它启动和结束时触发的两个事件，如表 5-5 所示。

表 5-5　Application 对象的事件及说明

| 事　件 | 说　明 |
|---|---|
| OnStart | 当 ASP 启动时触发，在用户请求的网页执行之前以及任何用户创建 Session 对象之前。用于初始化变量、创建对象或运行其他代码 |
| OnEnd | 当 ASP 应用程序结束时触发。在最后一个用户会话已经结束并且该会话的 OnEnd 事件中的所有代码已经执行之后发生。其结束时应用程序中存在的所有变量被取消 |

4)　Session 对象

可以使用 Session 对象存储特定用户会话所需的信息。这样当用户在应用程序的 Web 页之间跳转时，存储在 Session 对象中的变量将不会丢失，而是在整个用户会话中一直存在下去。当用户请求来自应用程序的 Web 页时，如果该用户还没有会话，则 Web 服务器将自动创建一个 Session 对象。当会话过期或被放弃后，服务器将终止该会话。Session 对象最常见的一个用法就是存储用户的首选项。例如，如果用户指明不喜欢查看图形，就可以将该信息存储在 Session 对象中。

其使用语法为：

```
Session.collection|property|method
```

Session 对象提供了 4 个属性，这些属性及说明如表 5-6 所示。

表 5-6　Session 对象的属性及说明

| 属　性 | 说　明 |
| --- | --- |
| CodePage | 读/写。整型。定义用于在浏览器中显示页内容的代码页(Code Page)。代码页是字符集的数字值，不同的语言和场所可能使用不同的代码页。例如，ANSI 代码页 1252 用于美国英语和大多数欧洲语言，代码页 932 用于日文字 |
| LCID | 读/写。整型。定义发送给浏览器的页面地区标识(LCID)。LCID 是唯一的标识地区的一个国际标准缩写，如 2057 定义当前地区的货币符号是“£”。LCID 也可用于 FormatCurrency 等语句中，只要其中有一个可选的 LCID 参数。LCID 也可在 ASP 处理指令<%......%>中设置，并优先于会话的 LCID 属性中的设置 |
| Session ID | 只读。长整型。返回这个会话的标识符，创建会话时该标识符由服务器产生。在父 Application 对象的生存期内是唯一的，因此当一个新的应用程序启动时可重新使用 |
| Timeout | 读/写。整型。为这个会话定义以分钟为单位的超时周期。如果用户在超时周期内没有进行刷新或请求一个网页，该会话结束。在各网页中根据需要可以修改。默认值是 10min，在使用率高的站点上该时间应更短 |

5)　Server 对象

Server 对象提供对服务器上的方法和属性的访问。其中，大多数方法和属性是作为实用程序的功能服务的。

其使用语法为：

```
Server.property|method
```

Server 对象的唯一一个属性用于访问一个正在执行的 ASP 网页的脚本超时值，如表 5-7 所示。

表 5-7　Server 对象的属性及说明

| 属　性 | 说　明 |
| --- | --- |
| ScriptTimeout | 整型。默认值为 90。设置或返回页面的脚本在服务器退出执行和报告一个错误之前可以执行的时间(秒数)。达到该值后将自动停止页面的执行，并从内存中删除包含可能进入死循环的错误的页面或者是那些长时间等待其他资源的网页。这会防止服务器因存在错误的页面而过载。对于运行时间较长的页面需要增大这个值 |

6)　ObjectContext 对象

可以使用 ObjectContext 对象提交或放弃一项由 Microsoft Transaction Server (MTS) 管理的事务，它由 ASP 页包含的脚本初始化。

当 ASP 页包含@TRANSACTION 指令时，该页会在事务中运行，直到事务成功或失败后才会终止。

其使用语法为：

```
ObjectContext.method
```

### 5.2.1.2　JSP

JSP(Java Server Pages)是由 Sun Microsystems 公司倡导，许多公司共同参与建立的一种

动态网页技术标准。在传统的网页 HTML 文件(*.htm、*.html)中加入 Java 程序片段(Scriptlet)和 JSP 标签，就构成了 JSP 网页(*.jsp)。Web 服务器在遇到访问 JSP 网页的请求时，首先执行其中的程序片段，然后将执行结果以 HTML 格式返回给客户。程序片段可以操作数据库、重新定向网页以及发送 E-mail 等，这就是建立动态网站所需要的功能。所有程序操作都在服务器端执行，网络上传送给客户端的仅仅是得到的结果，对客户端浏览器的要求最低，可以实现无 Plugin、无 ActiveX、无 Java Applet，甚至无 Frame。

1. JSP 的特点

与 ASP 和 PHP 相比，JSP 具有下列优点。

1) 内容的生成和显示分离

使用 JSP 技术，Web 页面开发人员可以使用 HTML 或者 XML 标签来设计和格式化最终页面。还可以使用 JSP 标签或者小脚本来生成页面上的动态内容。

2) 强调可重用的组件

绝大多数 JSP 页面依赖于可重用的、跨平台的组件(JavaBean 或 EJB)来执行应用程序所要求的更为复杂的处理。

3) 采用标识简化应用开发

通过开发定制化标识库，JSP 技术是可以扩展的。第三方开发人员和其他人员可以为常用功能创建自己的标识库。

4) 健壮性与安全性

由于 JSP 页面的内置脚本语言是基于 Java 编程语言的，而且所有的 JSP 页面都被译成 Java Servlet，所以 JSP 页面就具有 Java 技术的所有优点，包括健壮的存储管理和安全性。

5) 良好的可移植性

作为 Java 的一部分，JSP 拥有 Java 编程语言“一次编写，各处运行”的特点。

6) 企业级的扩展性和性能

在与 Java 2 平台、J2EE 和 EJB 技术整合时，JSP 页面将提供企业级的扩展性和性能。

2. JSP 程序页面

下面是 JSP 的一个应用实例，主要完成日期对象的相关操作，首先获取系统当前时间，然后重新设置系统时间，将系统时间设置为 2008 年北京奥运会开始的时间。

```
<%@ page contentType="text/html; charset=GB2312" import = "java.util.*" %>
<HTML>
<HEAD>
<TITLE>日期对象各时间段的取得与设置</TITLE>
</HEAD>
<BODY>
<CENTER>
<FONT SIZE = 5 COLOR = BLUE>日期对象各时间段的取得与设置</FONT>
</CENTER>
<HR>
<P></P>
<%                //声明 Date 对象变量，并建立 Date 变量
Date date = new Date();
```

```
%>
当前系统日期为<Font color = red>
<%= date.getYear() + 1900%>/
<%= date.getMonth() + 1%>/
<%= date.getDate()%>
</Font><P></P>
当前系统时间为<Font color = red>
<%= date.getHours()%>:
<%= date.getMinutes()%>:
<%= date.getSeconds()%>
</Font><P></P>
<%
date.setYear(2008);     //将年设置为 2008 年
date.setMonth(8);       //将月设置为 8 月
date.setDate(8);        //将日设置为 8 日
date.setHours(8);       //将小时设置为 8 时
%>

重新设置的新时间为<Font color = red><%= date%></Font>是北京奥运会开始的时间。

</BODY>
</HTML>
```

该 JSP 页面经过 JSP 服务器解释在客户浏览器上显示的结果如图 5-4 所示。




图 5-4　简单的 JSP 执行结果

3. JSP 技术的未来

JSP 技术被设计为一个开放的、可扩展的建立动态 Web 页面的标准。通过与业界领袖的合作，SUN 保证 JSP 规范的开放性和可移植性，可以使用任意客户机和服务器平台，在任何地方编写和部署它们。将来工具供应商和其他厂商将通过为专门的功能提供客户化的标识库而扩展平台的功能。

#### 5.2.1.3　PHP 和 ADO 数据库编程

1. PHP

PHP(Professional Hypertext Preprocessor)是一种服务器端 HTML 嵌入式脚本描述语言，目前正式发布的最高版本为 4.04。服务器端脚本技术又分为嵌入式与非嵌入式两种，PHP

是嵌入式的，如 ASP。它是一种功能非常强大的、面向 Internet/Intranet 的编程语言，可以开发动态交互的 Web 应用程序，可在多种系统平台和多种 Web 服务器中使用，是真正的跨平台、跨服务器的开发语言。

PHP 语言的主要特征如下。

(1) 免费，轻巧快速，真正跨平台。

(2) PHP 是一种遵守 GNU 条约的软件。根据此条约，所有用户都可以免费使用 PHP 并可以得到它的源代码，还可以在源代码上进行修改和完善，开发成适合自己使用的新的版本。

(3) 易学易用。因为 PHP 3.0 以上版本是用 C 语言实现的，而且它自身的语法风格与 C 语言极其相似，有许多的语句、函数 PHP 与 C 是完全相同的。

(4) 具有十分强大的数据库操作功能，可直接连接多种数据库，并完全支持 ODBC。这一特点是其他脚本语言所不能比拟的。

(5) 可以嵌入 HTML 中。当使用者使用经典程序设计语言(如 C 或 Pascal 编程)时，所有的代码必须编译成一个可执行的文件，然后该可执行文件在运行时为远程的 Web 浏览器产生可显示的 HTML 标记。

2. ADO 数据库编程

微软公司的 ADO(ActiveX Data Objects)是一个用于存取数据源的 COM 组件。它是编程语言和统一数据访问方式 OLE DB 的一个中间层，允许开发人员编写访问数据的代码、到数据库的连接，而不用关心数据库的实现。ADO 的操作步骤如下。

(1) 打开连接。ADO 打开连接的主要方法是使用 Connection.Open 方法。另外，也可在同一个操作中调用快捷方法 Recordset.Open 打开连接并在该连接上发出命令。

(2) 创建命令。ADO 可提供简易灵活的方法，在单个步骤中创建 Parameter 对象并将其追加到 Parameter 集合。

```
cmd.Parameters.Append cmd.CreateParameter-
"au lname", adVarChar, adtnput, 40, "Ringer"
```

(3) 执行命令。返回 Recordset 的方法有 3 种，即 Connection.Execute、Command.Execute 和 Recordset.Open。以下是它们的 Visual Basic 语法：

```
Connection.Execute(CommandText, RecordsAffected, Options)
Command.Execute(RecordsAffected, Parameters, Options)
Recordset.Open Source, ActiveConnection, CursorType,LockType,Options
```

(4) 操作数据。有多种方法可在 Recordset 中显式移动或“定位”(Move 方法)。一些方法(Find 方法)在其操作的附加效果中也能够做到。此外，设置某个属性(Bookmark 属性)同样可以更改行的位置。Filter 属性用于控制可访问的行(这些行是“可见的”)。Sort 属性用于控制所定位的 Recordset 行中的顺序。Recordset 有一个 Fields 集合，它是在行中代表每个字段或列的 Field 集，可从 Field 对象的 Value 属性中为字段赋值或检索数据。作为选项，可访问大量字段数据(GetRows 和 Update 方法)。使用 Move 方法从头至尾对经过排序和筛选的 Recordset 进行定位。

(5) 更新数据。对于添加、删除和修改数据行，ADO 有两个基本概念。第一个是不立

即更改 Recordset，而是将更改写入内部“复制缓冲区”；第二个是只要声明行的工作已经完成，则将更改立刻传播到数据源(“立即”模式)，或者只是收集对行集合的所有更改，直到声明该行集合的工作已经完成(“批”模式)。这些模式将由 CursorLocation 和 LockType 属性控制。

(6) 结束更新。ADO 检测到“冲突”并报告错误，如果错误存在，它们会被错误处理例程捕获。可使用 adFilterConflictingRecords 常数对 Recordset 进行筛选，将冲突行显示出来。要纠正错误只需打印作者的姓和名(au fname 和 au-lname)，然后回卷事务，放弃成功的更新。由此结束更新。

## 5.2.2　典型例题分析

**例 1**　阅读下列说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。(2015 年 5 月下午试题四)

**【说明】**

某学生信息管理系统的网站后台管理主页如图 5-5 所示。




**图 5-5　学生信息管理系统网站后台管理主页**

**【问题 1】**(7 分)

以下是该管理系统后台管理主页部分的 HTML 代码，请根据图 5-1，从以下备选答案内为程序中(1)～(7)处空缺部分选择正确答案。

```
<html>
<head>
<title>___(1)___<title>
</head>

<%
    If___(2)___("admin")=""
    Then___(3)___Redirect ("login.asp")
```

```
    (4)
%>
<frameset  (5)  ="71,*" framespacing="0" border="0" frameborder="0">
<frame  (6)  ="head.asp" scrolling="no" name="head" noresize>
<frameset  (7)  ="152,*">
<frame src="menu.asp">
<frame src="main.asp" name="main" scrolling="yes" noresize>
</frameset>
</frameset>
……
</html>
```

(1)～(7)的备选答案：

A．cols　　B．else　　C．Rows　　D．response

E．Src　　F．session　　G．设为首页　H．后台管理

【问题 2】(10 分)

以下是该管理系统学生信息录入页面部分的 HTML 代码，请根据图 5-1，从以下备选答案内为程序中(8)～(15)处空缺部分选择正确答案。

```
<html>
……
<script language="JavaScript">
 (8)  check()
{
    if(forma. (9) .value=="")
    {
        alert("请输入学生姓名！");
        forma.name_xs.focus();
        return  (10) ;
    }
    ……
    return  (11)  ;
}
</script>
……
<form action=" " method="post"  (12)  ="return check();">
    <table>
    <tr>
      <td heigh="21" colspan="2">[<strong>添加学生信息</strong>]
         <font color="#0000FF"></font></td>
    </tr>
    <tr>
      <td width="19%" height="20">学生姓名:</td>
     <td width="81%"><input name="name_xs" type="  (13)  "id="name_cnxdb"
onkeydown="next()"></td>
    </tr>
……
    <tr align="center">
    <td><input type="  (14)  " value="增加">
    <input type="  (15)  "value="重写"></td>
……
</html>
```

(8)～(15)的备选答案：

A. false　B. Function　C. name_xs　D. onsubmit
E. true　F. reset　G. submit　H. text

**分析：**

**【问题 1】**

根据图示网页及提供的程序代码，该网站主页面中的(1)空是网页的标题，(2)～(4)空属于 ASP 编程中的基础知识。(5)～(7)空考查的是 HTML 中表单设置的基本知识。所以代码如下：

```
<html>
<head>
<title>后台管理</title>
</head>
<%
  If session("admin")=""then response.Redirect ("login.asp")
   else
%>
<frameset  cols ="71,*" framespacing="0" border="0" frameborder="0">
<frame  src ="head.asp" scrolling="no" name="head" noresize>
  <frameset  rows  ="152,* ">
  <frame src="menu.asp">
  <frame src="main.asp" name="main" scrolling="yes" noresize>
</frameset>
</frameset>
……
</html>
```

**【问题 2】**

其中，check()为函数名，所以可以判断(8)空应填写 function，(9)～(11)空判别用户输入表单值的状况，(12)～(15)空是表单处理程序。所以该程序代码如下：

```
<html>
……
<script language="JavaScript">
function  check()
    {
    if (forma. name_xs.value==" ")
    {
        alert("请输入学生姓名!");
        forma.name_xs.focus();
        return  false;
    }
……
return  true;
</script>
……
<form action=" " method="post" onsubmit ="return check();">
```

```
    <table>
    <tr>
        <td height="21" colspan="2">[<strong>添加学生信息</strong>]
        <font color="#000FF"> </font></td>
    </tr>
    <tr>
        <td width="19%" height="20"> 学生姓名:</td>
        <td width="81%"><input name="name_xs" type=" text " "id=" name_cnxdb"
        onkeydown="next()"></td>
    </tr>
……
    <tr align="center">
    <td><input type=" submit " value="增加">
    <input type =" reset  " value="重写"></td>
……
</html>
```

答案:

【问题 1】

(1) H (2) F (3) D (4) B (5) C (6) E (7) A

【问题 2】

(8) B (9) C (10) A (11) E (12) D (13) H (14) G (15) F

例 2 阅读以下说明，回答问题 1 至问题 5。(2015 年 11 月下午试题四)

【说明】

某公司使用 ASP 开商务网站，网页制作过程使用了 CSS 技术，该网站具有商品介绍、会员管理、在线支付和物流管理等功能，采用 SQL Server 数据库，数据库名称为 business，其中用户表名称 name，其结构如表 5-8 所示。

表 5-8 用户表中字段说明

| 字 段 名 | 类 型 |
|---|---|
| UserName | char |
| Password | char |
| Usergrade | char |

其中，Usergrade 仅有两个有效值：m 表示会员；b 表示非会员。

【问题 1】(3 分)

在该网站 index.asp 文档中使用了<style type= "text/css">语句。其中 CSS 是指__(1)__，它是一种__(2)__样式描述格式，能够保证文档显示格式的一致性，CSS 本身__(3)__XML 的语法规范。

(1) 备选答案:

A. 扩展样式单　　　　B. 层叠样式单

(2) 备选答案:

A. 静态　　　　B. 动态

(3)　备选答案：

A．遵从　　B．不遵从

**【问题 2】**(3 分)

该网站数据库连接代码如下，根据题目要求在备选项中选择正确的答案。

```
<%
set conn=__(4)__.createobject("adodb.connection")
conn.provider="sqloledb"
provstr="server=127.0.01; database=__(5)__;uid=sa; pwd=9857452"
__(6)__.open provstr
%>
```

(4)～(6)备选答案：

A．applicaton　B．business　C．provstr

D．conn　E．name　F．server

**【问题 3】**(5 分)

该网站只对会员开放购物车模块，当非会员单击购物车模块时系统自动跳转至会员注册页面，会员用户单击购物车模块时直接进入购物车模块的首页。其中购物车模块的首页为 main.asp，用户登录时判断页面是 ChkLogin.asp，会员注册页面为 Register.asp。

① ChkLogin.asp 的部分代码如下，请根据题目要求补充完整：

```
<!--#include file=conn.asp-->
<%
    ……
    usname=replace(trim( __(7)__ ("usename")),"`","")
    ……
    sql="select*from __(8)__ where password=`"&password"` and userName=
&username&"`"
rs.open sql,conn,1,1
if__(9)__(rs.bof and rs.eof) then
    if password=rs("password") then
        session("username")=rs("username")
        session("usergrade")=rs("usergrade")
    ……
%>
```

(7)～(9)备选答案：

A．not　B．connection　C．name

D．movefirst　E．execute　F．request

G．connectionString　H．dim　I．mappath

② main.asp 的部分代码如下，请根据题目要求补充完整：

```
<%
If __(10)__<>"m" then
response.__(11)__"Register.asp"
end if
%>
```

```
<html>
……
</html>
```

(10)、(11)备选答案：

A．session("Username")　　B．session("Usergrade")　　C．run

D．redirect　　E．write　　F．coolaie

**【问题 4】**

该网站举办购物优惠活动，希望用户打开网站首页时弹出提示窗口。首页 Index.asp 中部分代码如下，请根据题目要求补充完整：

```
<html>
<head>
……
<script language="javascript">
…
func…tion win()
{
windows.__(12)__("yh.html","newwindow", "height=100, width=400")
}
……
</script>
</head>
<body__(13)__ = "win()">
……
</body>
</html>
```

(12)、(13)备选答案：

A．command　　B．connection　　C．read

D．onload　　E．open　　F．close

**【问题 5】**

① 在 ASP 中，__(14)__是 Session 对象的方法。

(14)备选答案：

A．Lock　　B．CreateObject　　C．Abandon　　D．Redirect

② 在以下组合中，__(15)__不能开发出动态网页。

(15)备选答案：

A．TML+JSP　　B．HTML +XML　　C．XML+JSP　　D．XML+ASP

**分析：**

**【问题 1】**本问题主要考查考生对 CSS 的掌握和应用。

CSS(Cascading Style Sheets，层叠样式表)是一种用来表现 HTML(标准通用标记语言的一个应用)或 XML(标准通用标记语言的一个子集)等文件样式的计算机语言。

CSS 目前最新版本为 CSS3，是能够真正做到网页表现与内容分离的一种样式设计语言。相对于传统 HTML 的表现而言，CSS 能够对网页中的对象的位置排版进行像素级的精

确控制，支持几乎所有的字体、字号样式，拥有对网页对象和模型样式编辑的能力，并能够进行初步交互设计，是目前基于文本展示最优秀的表现设计语言。CSS 能够根据不同使用者的理解能力，简化或者优化写法，针对各类人群，有较强的易读性。它是一种静态样式描述格式，能够保证文档显示格式的一致性，CSS 不遵从 XML 的语法规则，而 XSL 遵从 XML 的语法规则。

**【问题 2】**server.createobject 方法用于创建某个 ASP 对象，根据题意，数据库名称为 business，所以 database=business。

第(4)空选择 server，创建一个数据库连接实例。

第(5)空选择 business，因为数据库名称为 business。

第(6)空选择 conn，连接数据库。

**【问题 3】**

① 第(7)空选择 request，获取表单的 username 值赋值给变量 username。

第(8)空选择 name，从用户表 name 中查找。

第(9)空选择 not，在查询数据库时这句话可判断记录集是否为空，如果为空 not(rs.bof and rs.eof)就是假值。程序就会不做下面的动作。

② 第(10)空为 Session("Usergrade")，不是会员。

第(11)空为不是的话就重定向到注册页面。

**【问题 4】**

window.Open()用于打开一个新的浏览器窗口或查找一个已命名的窗口。onload 是页面加载完成后执行的动作，一般写在 body 里面。onload 事件会在页面或图像加载完成后立即发生。

第(12)空答案为 open，打开窗口。

第(13)空答案为 onload，onload 事件在页面载入完成后立即触发。

**【问题 5】**

Session 对象的常见属性和方法包括 SessionID、Timeout、IsNewSession、Clear()、Abandon()。要开发动态网页，可使用 ASP、JSP、PHP 等动态网页技术，HTML 和 XML 不能开发出动态网页。

**答案：**

**【问题 1】**(1) B　(2) A　(3) B

**【问题 2】**(4) F　(5) B　(6) D

**【问题 3】**(7) F　(8) C　(9) A　(10) B　(11) D

**【问题 4】**(12) E　(13) D

**【问题 5】**(14) C　(15) B

**例 3**　阅读下列说明，回答问题 1 和问题 2，将解答填入答题纸的对应栏内。(2016 年 5 月下午试题四)

**【说明】**

某公司用 ASP+Access 数据库开发了学生管理系统，用户登录界面如图 5-6 所示。

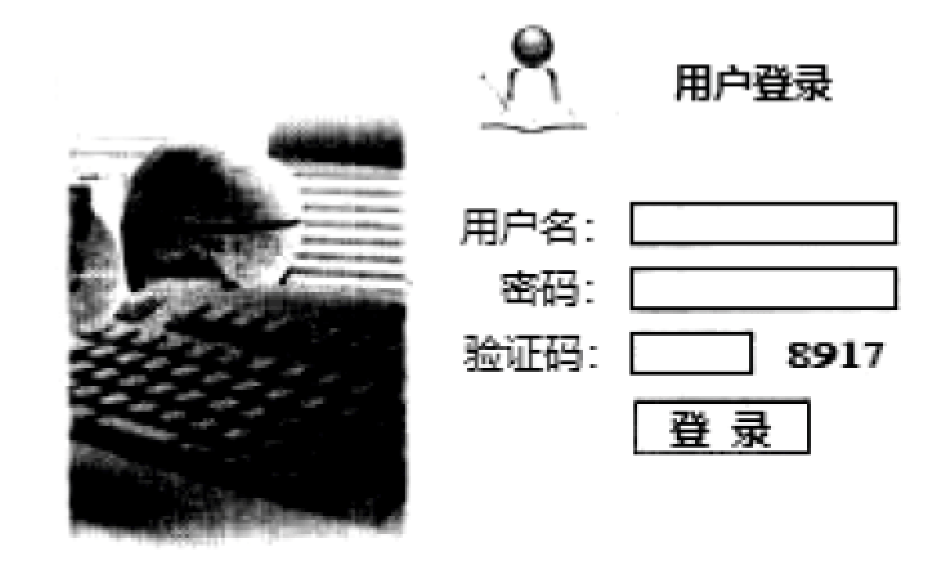



图 5-6　学生管理系统

【问题 1】

下面是该系统用户登录界面 login.asp 的部分代码，其中验证码使用 vericode.asp 文件生成。请根据题目说明补充完整。

```
<html xmlns="http://www.w3.org/1999/xhtml">
  (1)
<title>学生信息管理系统</title>
<script language="JavaScript”>
<!--
function chk(theForm)
{
if(theForm.  (2)  .value="")
{
         alert("请输入用户名! ");
         theForm.user_name.focus();
         return(  (3)  );
      }
     if(theForm.  (4)  .value=="")
      {
         alert("请输入密码! ");
         theForm.user_pwd.focus();
         return(false);
      }
       (5)  true;
}
      ……//省略验证码检测部分代码
      -->
</script>
</head>
<body>
<table cellSpacing=1 cellPadding=5 width=460 border=0>
<FORM action="check.as? action=login"
method=(6)onSubmit="returnchk(this)">
……
<tr>
<td align=right width=60 height=30>用户名:</td>
<td height=30><input type=  (7)  name=user_name></td></tr>
<tr>
```

```
<td align=right height=30>密码:</td>
<td height=30><input type= __(8)__ name=use_pwd></td></tr>
<tr>
<td align=right>验证码: </td>
<td><input maxlength __(9)__ name=veri_code><imgsrc="vericode.asp"
border='0' onClick="this.src='__(10)__"" alt='点击刷新'/></td></tr>
<tr align=middle>
<td colSpan=2 height=40><inputtype=__(11)__value="登录">
</td>
……
</body>
</html>
```

【问题 2】

下面是登录系统中 check.asp 文件的部分代码，请根据 login.asp 代码将其补充完整。

```
<%
username=trim(request("user_name"))
password=trim(request("user_pwd"))
setrs=server.create object("adodb.recordset")
sql="select * from admin where username=""&username&"" and password=
""&md5(password)&""
    __(12)__.opensql,conn,1,3
if rs.eofthen
response.write"<center>"&username&"用户名或密码错误，请重新输入！"
else
……
session("user_name")=request("usre_name")
response.__(13)__"index.asp"
end if
……
%>
```

**分析：**

【问题 1】

该题目要求制作一个用户登录界面，并对用户输入的数据进行检测。当用户名或者密码为空时，返回要求用户输入用户名或密码的提示，并将光标定位在用户名和密码的输入框内。该段代码应放置于<head></head>标签内。在<body></body>标签对内是登录界面设计，包括输入框的类型和属性等，引用 vericode.asp 文件生成验证码。

【问题 2】

该题目是对用户输入的用户名和密码的正确性进行验证。当用户名和密码不匹配时，弹出相应提示，要求用户重新输入，当输入正确时将跳转到登录成功页面。

**答案：**

【问题 1】

(1) <head>　(2) user_name　(3) false　(4) user_pwd　(5) return　(6) post

(7) text　(8) password　(9) 4　(10) vericode.asp　(11) submit

【问题 2】

(12) rs　　　(13) redirect

例 4　阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内口。(2016 年 11 月下午试题四)

【说明】

某学校新生入学后进行信息登记，其登记页面和登记后信息显示页面分别如图 5-7 和图 5-8 所示。

学生档案

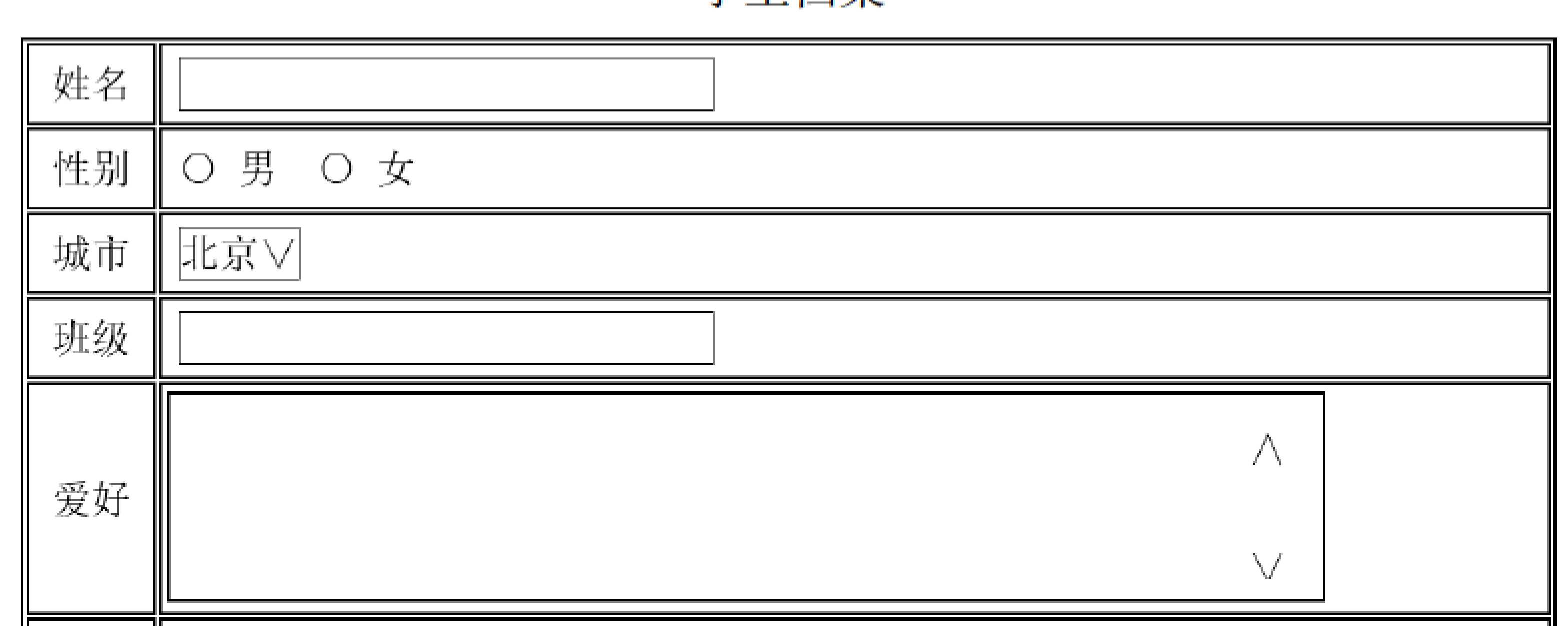



图 5-7　登记页面

你是第 10 位登记者

| 姓名 | 性别 | 城市 | 班级 | 爱好 |
|---|---|---|---|---|
| 李明 | 男 | 上海 | 五班 | 足球、音乐 |

图 5-8　登记后信息显示页面

【问题 1】

以下是图 5-7 所示的 index.asp 页面的部分代码，请仔细阅读该段代码，将(1)～(9)的空缺代码补齐。

index.asp 文档的内容如下：

```
<title>学生档案</title>
<body>
<div aljgn=" (1) ">
<hl><strong>学生档案</stro><hl>
</div>
<form id="form1" name="form1" method=" (2) " action=show.asp">
     <table width="485" border="1" align="center">
     <tr>
     <td>姓名</td>
     <td><label for="name"></label>
     input type=" (3) "name="name"id="name"/></td>
```

```
</tr>
<tr>
<td>性别< / td>
<td><input type="(4)" name="sex" id="radio" value="男" />
<label for="sex">男
<input type="radio" name="sex" id="radio2" value=” 女" />
女</label></td>
</tr>
<tr>
<td>城市</td>
<td><label for="city"></label>
<(5) name="city" id="city">
<option  value="北京"  selected="(6)">北京</option>
<option value="上海">上海</option>
<option value="广州>广州</option>
</select></td>
</tr>
<tl>
<td>班级</td>
<td><label for"class"></label>
<input type-"text" name="class" id="class"/></td>
</tr>
<tr>
<td>爱好</td>
<td><label for="favorite"></label>
<(7)name="favorite" id="favorite" cols="45" rows= "5"></textarea></td>
<tr>
<tr>
<td> </td>
<td><input type="(8)" name="'button" id="button" value="提交" />
<input type="(9)name="'button2" id="button2" value="重新填写"/></td>
</tr>
</table>
</form>
</body>
</html>
```

(1)～(9)备选答案：

A．submit　　B．selected　　C．post　　D．reset　　E．radio

F．text　　G．center　　H．textarea　　I．select

**【问题 2】**

学生输入信息并提交后，系统将回显学生信息，并显示登记位次。下面是显示学生登记位次的部分代码，请根据图 5-8 将下面代码补充完整。

```
<%
    Whichfile=server.mappath("register.txt")
    set fs=server.(10)("Scripting.FileSystemObject")
    set thisfile=fs.opentextfile(whichfile)
    visitors=(11).readline
```

```
        thisfile.close
        response.Write("<center><font size=5>你是第"&(12)&位登记者
</font></center>”)%>
        ……//省略页面显示部分代码
        <%
        visitors=visitors+1
        Set out=fs.(13)(whichfile)
        (14).writeLine(visitors)
        out.close
        set fs=(15)
%>
```

(10)～(15)备选答案：

A．thisfile　　B．visitors　　C．nothing

D．CreatObject　　E．out　　F．createtextfile

分析：

【问题 1】

本问题主要考查 ASP 的一些基本设置命令。

(1) 将标题“学生档案”居中，所以选择 center。

(2) method="post"表示表单中的数据"post"方式传递，即发送的数据直接发送到服务器端。action 是提交动作，即提交过去的页面交给 show.asp 来处理。

(3) 表示输入类型是文本，如登录输入用户名，注册输入电话号码、电子邮件、家庭住址等。

(4) 表示输入类型是单选框。

(5) 表示带有 name 属性的下拉列表。

(6) 表示默认选择的表项。

(7) 表示输入类型为输入框。

(8) 表示输入类型是“提交”。

(9) 表示输入类型是“重置”。

【问题 2】

本问题主要考查 ASP 创建对象的相关命令。

(10) 创建 FileSystemObject 对象实例 fs。

(11) 读取计数文件的内容。

(12) 显示计数变量 vistors 的数值。

(13) 创建输出文件对象。

(14) 在输出文件对象中写入数值。

(15) 关闭对象。

答案：

【问题 1】

(1) G　(2) C　(3) F　(4) E　(5) I　(6) B　(7) H　(8) A　(9) D

【问题 2】

(10) D　(11) A　(12) B　(13) F　(14) E　(15) C

**例 5**　阅读下列说明，回答问题 1 和问题 2，将解答填入答题纸的对应栏内。(2017 年 5 月下午试题五)

**【说明】**

某网站涉及了一个留言系统，能够记录留言者的姓名 IP 地址以及留言时间。撰写留言页面如图 5-9 所示。表 5-9 所列为利用 Microsoft Access 创建的数据库 lyb。

撰写留言




**图 5-9　留言页面**

**表 5-9　address 数据表结构**

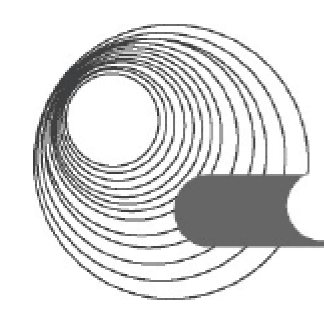
| 字段名称 | 数据类型 | 字段作用 |
| --- | --- | --- |
| name | 文本 | 留言人姓名 |
| ly | 备注 | 留言内容 |
| ipadd | 文本 | 留言人 IP 地址 |
| hf | 备注 | 回复内容 |
| lytime | 日期/时间 | 留言时间 |

**【问题 1】**

以下为 write.asp 页面的部分代码，请仔细阅读该段代码，将(1)~(10)的空缺代码补齐。

```
Set MM_editCmd=Serve.CreateObject("ADODB.Command")
MM_editCmd.ActiveConnection=MM_Connbook STRING
MM_editCmd.CommandText ="INSERT INTO lyb (name,(1),ipadd,lytime)
VALUES(?,?,?,?)"
MM_editCmd.Prepared =true
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param1",202,1,255,
Request.Form("name"))'adVarWChar
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param2",203,1,536
870910,Request.From("ly"))' adlongvarwchar
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param3",202,1,255,
(2).Form("ipadd"))'adVarWChar
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param4", 135, 1,-1,
MM_IIF(Request.Form("lytime"),Request.Form"lytime"),null))'adDBTimeStamp
MM_editCmd.Execute
MM_editCmd.AditCmd,ActiveConnection.Close

<body>
```





```
<%IP=Request("REMOTE_ADDR")%>
<P><strong>撰写语言
</strong></p>
</hr>
<form ACTION="<%=MM_editAction%>"METHOD="(3)"id="form1"name="form1">
<table width="500"borde="1"align="center"
<tr>
<td width="94"align="right">您的姓名</td>
<td width="390"align="left"><label for ="name"></label>
<input type="test"name"id="name"/></td>
</tr>
<tr>
<td align="right">您的留言</td>
<td align="left"><label for ="ly"></label>
<(4)name="ly"cols ="50"rows="5"id="ly"></textarea></td>
</tr>
<tr>
<td align="center"><a herf ="(5).asp">返回首页</a></td>
<td align="center"><input name="(6)"type="hidden"id="ipadd"value ="<%
=ip%>"/>
<input name="lytime"type="(7)id="lytime"value="<%=(8)0%>"/>
<input type="(9)name="button"id="button"value="提交"/><label for="radio"
<input type="(10)"name="button2"id="button"value="重置"/>
</label></td>
<tr>
</table>
```

(1)～(10)备选答案：

A．submit　B．ipadd　C．ly　D．reset　E．index
F．post　G．now　H．textara　I．Request　J．hidden

【问题 2】(2 分)

图 5-10 是留言信息显示页面。系统按照 B 值从大到小的顺序依次显示留言信息，单击图 5-9 中的“返回首页”按钮，将返回到此页面。下方代码为所示页面文件 index.asp 的部分代码，请仔细阅读该段代码，将(11)～(15)的空缺代码补齐。

| | | |
|---|---|---|
| 留言：2 | 姓名：刘怡 | IP：202.118.0.12 |
| 留言内容 | 有事咨询，请提供联系方式。 | |
| | 留言时间：2017/1/24 21:54:18 | |
| 回复内容 | | |

图 5-10　留言页面图




图 5-10　留言页面图(续)

```
Set Recordset1_cmd = Server.CreateObject ("ADODB.Command")
Recordset1 cmd.ActiveConnection = MM Connbook STRING
Recordset1_cmd.CommandText = "SELECT * FROM lyb ORDER BY (11) -DESC"
Recordset1_cmd.Prepared =true

<body>
<%
While((Repeat1_numRows<>0)AND(NOT Recordet1.EOF))
%>
<p>  </p>
<table width="500"border="1">
<tr>
<td width="108">留言：<%=(Recordset1.Fields.Item("ID").Value)%></td>
<td width="196">留言：<%=(Recordset1.Fields.Item(" (12) ").Value)%></td>
<td width="174">IP：<%=(Recordset1.Fields.Item(" (13) ").Value)%></td>
</tr>
<tr>
<td rowspan="2">留言内容</tb>
<td colspan="2"><label for "textdield"></label>
<textarea name="textfield" cols="45" rows="5"
id="textfield"><%=(Recordset1.Fields.Item("ly").Value)%><Itextarea></td>
</tr>
<tr>
<td colspan="2"> 留言时间：<%=(Recordset1.Fields.Item(" (14) ").Value)%></td>
</tr>
<tr>
<td>回复内容</td>
<td colspan="2"><label for="textfield2"></label>
<textarea name="textfield2" cols="45" rows="3"
id="textfield2"><%=(Recordset1.Fields.Item
(" (15) ").Value)%></textarea></td>
</tr>
</table>
```

(11)～(15) 备选答案：

A. hf　B. ipadd　C. ID　D. name　E. lytime

分析：

【问题 1】

(1) ly 表示留言的内容。

(2) request.Form 命令可用于从表单取回信息。

(3) post 请求提交数据。

(4) <textarea> 元素用于创建文本域。

(5) index.asp 表示首页。

(6) ppadd 留言人的 IP 地址。

(7) hidden 隐藏。

(8) now 现在的时间。

(9) submit 表示输入类型是“提交”。

(10) reset 表示输入类型是“重置”。

【问题 2】

(11) 以留言 ID 按降序排列。

(12) 返回留言人姓名。

(13) 返回留言 IP 记录。

(14) 返回留言时间记录。

(15) 返回回复内容记录。

答案：

【问题 1】

(1) C　(2) I　(3) F　(4) H　(5) E

(6) B　(7) J　(8) G　(9) A　(10) D

【问题 2】

(11) C　(12) D　(13) B　(14) E　(15) A

例 6　阅读以下说明，回答问题 1 和问题 2，将解答填入答题纸对应的解答栏内。(2017 年 11 月下午试题四)

【说明】

访问某聊天系统必须先注册，然后登录才可进行聊天。图 5-11 所示为注册页面，注册时需要输入用户名和密码及性别信息，数据库将记录这些信息。




图 5-11　注册页面

表 5-10 为利用 Microsoft Access 创建的数据库 msg，数据库记录用户名、密码、性别、登录时间、IP 地址及状态信息。

表 5-10　Access 数据表结构

| 字段名称 | 数据类型 | 字段作用 |
| --- | --- | --- |
| user | 文本 | 用户名 |
| upass | 文本 | 用户密码 |
| sex | 文本 | 用户性别，male 和 female |
| t | 日期/时间 | 登录时间 |
| ip | 文本 | 登录 IP |
| zt | 数字 | 状态，1 为在线，0 为退出 |

index.asp 文档的内容如下：

```
<html>
<head>
<title>投票程序</title>
<%
Set cnn=Server.CreateObject("ADODB.Connection")
Set rec=Server.CreateObject("ADODB.Rec")
```

**【问题 1】**

以下是图 5-11 所示页面的部分代码，请仔细阅读该段代码，将(1)～(6)的空缺代码补齐。

```
<%
Set MM_editCmd=Server.CreateObject("ADODB.Command")
MM-_editCmd.ActiveConnection=MM_connbbs_STRING
MM_editCmd.CommandText="INSERT INTO msg([user],upass,sex)VALUES(?,?,?)"
MM_editCmd.PrePared=true
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param1",202,1,225,
Request.Form("user"))'adVarWChar
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param2",202,1,225,
Request.Form("(1)"))'adVarWChar
MM_editCmd.Parameters.AppendMM_editCmd.CreateParameter("param3",202,1,225,
Request.Form("sex"))'adVarWChar
MM_editCmd.Execute
MM-_editCmd.ActiveConnection.Close
%>
<body>
<from ACTION="<%=MM_editAction%>"METHOD="(2)"id="form1" name="form1">
<p align="center">欢迎注册
</p>
<table width="500" border="0" align="center"cellpadding="1"cellspacing="2">
<tr><td><div align="right">请输入用户名</div></td>
<td>  <input type="text"name="(3)"id="user"/></td>
</tr><tr>
<td><div align="right">请输入密码</div></td>
<td>  <input type=" (4)"name="upass"id="upass"/></td>
```

```
</tr><tr>
<td><div align="right">重复输入密码</div></td>
<td>  <input type="text"name="pass2"id="pass2"/></td>
</tr><tr>
<td><div align="right">请输入性别</div></td>
<td> 
<input name="sex"type="radio"id="radio"value="(5)"/>
<lable for="sex">男
<input type="radio"name="sex"id="radio2"value="female"/>
女</label></td></tr><tr>
<input type="submit"name="button"id="button"value="提交"/>
<input type="(6)"name="button2"id="button2"value="重置"/></td></tr>
</table>
```

(1)～(6) 备选答案：

A．reset　B．male　C．post　D．text　E．user　F．upass

**【问题 2】**

用户注册成功后的登录页面如图 5-12 所示。系统检查登录信息与数据库存储信息是否一致，如果一致则转到登录成功页面 succ.asp；如果不一致则显示“警告：您输入的信息有误！”下面是信息显示页面的部分代码，请将下面代码补充完整。




图 5-12　注册用户登录页面

```
<%
set conn=server.createobject("adodb.connection")
conn.Open"Provider=Microsoft.Jet.OLEDB.4.0;Data source=C:\wwwroot\bbs.mdb"
    if request.form("user")<>""then
    u=request.form("user")
    p=request.form("upass")
    s=request.form("sex")
    set rs=server.createobject("adodb.recordset")
    rs.open "select" * from msg where(7)="&u&"and(8)="&p&"and
    sex="&s&"""",conn,1,3
    if.rs.(9)and rs.bof then
        response.(10) ("警告：您输入的信息有误！")
    else
        rs("t")=(11)()
        rs("(12)")=request.ServerVariables("remote_host")
        rs("zt")=1
        rs.update
```

```
        session("user")=u
        session("(13)")=s
        response.(14)"suss.asp"
    end if
rs.close()
set rs=nothing
end if
%>

<body>
    <form id="form1"name="form1"method="post"action="user.asp">
        <p align="center">欢迎登录</p>
    <div align="center"
    <td><div align="right">输入用户名</div></td>
    <td><label for="user"></label>
        <input type="text"name="user"id="user"/>
    </td>
    <td><div align="right">输入密码</div></td>
    <td>
        <label for="upass"></label>
        <input type="text"name="upass"id="upass"/>
    </td>
    <td>
        <div align="right">您的性别</div>
    </td>
    <td>
    <input name="sex"type="radio"id="radio"value="male"checked="(15)"/>
    <label for="sex">男
    <input type="radio"name="sex"id="radio2"value="female"/>女</label>
    </td>
    <td>
    </td>
    <td>
        <input type="submit"name="button"id="button"value="登录"/>
        <input name="button2" type="submit" id="button2" onclick="MM_goToURL
    ('parent','index.asp');return document.MM_returnValue"value="返回"/>
    </td>
    </tr>
```

(7)～(15)备选答案：

A. now　　B. ip　　C. checked　　D. eof　　E. upass
F. user　　G. write　　H. sex　　I. redirect

**分析：**

**【问题 1】**

(1) F，upass 表示请求用户密码字段。

(2) C，post 使用 post 方式提交。

(3) E，user 输入用户名到用户名字段。

(4) D，text 定义密码框中输入的格式为文本格式，密码可以是字母加数字的格式。

(5) B，male 选择性别为 male。

(6) A，reset 定义重置按钮。

**【问题 2】**

(7) F，user 提取用户输入的用户名字段中的用户名。

(8) E，upass 提取用户输入的密码字段中的密码。

(9) D，eof 数据库语言语法，用来判断数据库中是否有该数据。

(10) G，write 显示数据，对应 read 是读入数据。

(11) A，now 记录登录的时间是当前 now。

(12) B，ip 记录登录 IP 地址。

(13) H，sex 获取性别信息。

(14) I，redirect 基础语法知识，浏览器重新定位到另一个 URL 上，完成页面转换，需要 redirect 重定向。

(15) C，checked，checked 属性规定在页面加载时应该预先选定的 input 元素。

答案：

**【问题 1】**

(1) F

(2) C

(3) E

(4) D

(5) B

(6) A

**【问题 2】**

(7) F

(8) E

(9) D

(10) G

(11) A

(12) B

(13) H

(14) I

(15) C

## 5.2.3 同步练习

阅读以下说明，回答问题 1 至问题 3，将解答填入对应的解答栏内。

**【说明】**

某留言板采用 ASP+Access 开发，其后台管理登录页面如图 5-13 所示。留言板页面如图 5-14 所示。




图 5-13　后台管理登录页面

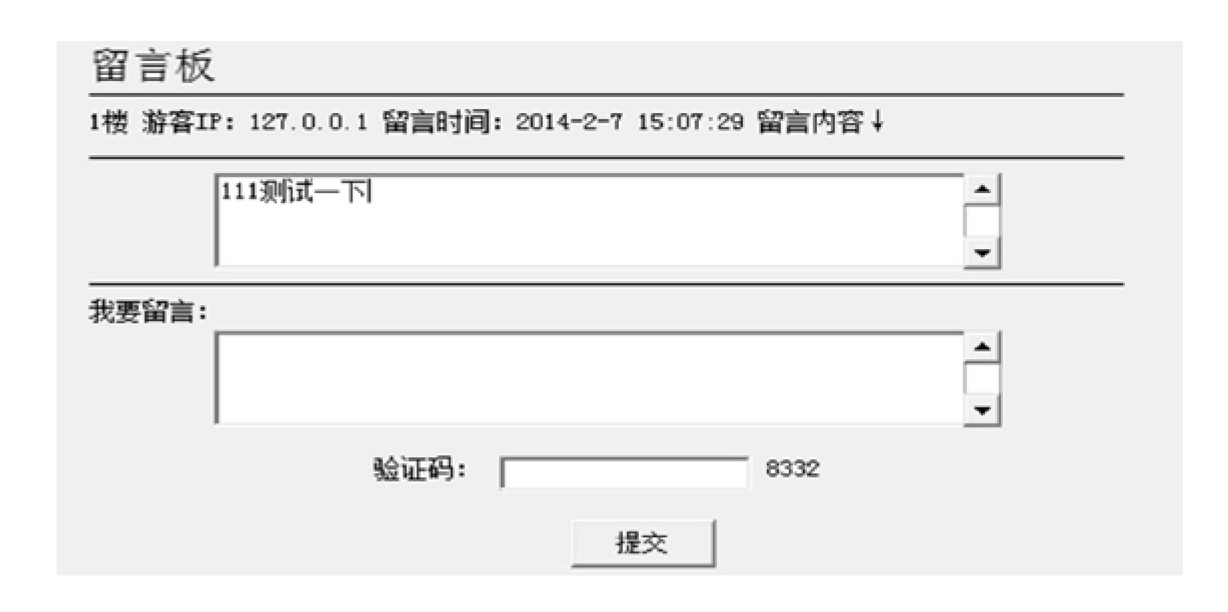



图 5-14　留言板页面

**【问题 1】**

以下是该网站主页部分的 HTML 代码，请根据图 5-13 将(1)～(8)的空缺代码补齐。

```
<!--# ___(1)___ file="conn.asp" -->
<html>
……
<div id="content" class="layout">
<div class="right_body">
< ___(2)___ name="guestbook" ___(3)___ ="post" ___(4)___ ="guestbook_add.asp">
<table class="table">
<tr>
<th width="60"> </th>
<td><label> </label> </td>
</tr>
<tr>
<th width="60"> </th>
<td><input name="title" type=" ___(5)___ " size="50"> </td>
</tr>
<tr>
<th> </th>
<td> < ___(6)___ name="body" cols="60" rows="5"> </textarea> </td>
</tr>
<tr>
<td colspan="2"> <p class="tj">
<input name="tj" type=" ___(7)___ " " ___(8)___ "="提交吧！">
</p></td>
</tr>
</table>
</form>
</div>
```

```
……
</html>
```

(1)~(8)的备选答案：

A．submit　B．form　C．text　D．textarea

E．include　F．action　G．method　H．value

【问题 2】

该网站在主页上设置了分页显示，每页显示 10 条留言，以下是该网站页面分页显示部分代码，请阅读程序代码，并将(9)~(15)的空缺代码补齐。

```
……
<%
Set rs = server.CreateObject("adodb.recordset")
 (9) ="select * from cont  (10)  by id desc"
rs.Open exect conn, 1, 1
if rs. (11)  Then
response.Write " 暂无留言！"
Else
rs.PageSize= (12)     "每页记录条数"
iCount= rs.RecordCount  "记录总数"
iPageSize=rs.PageSize
maxpage=rs.PageCount
page= request("page")
If Not IsNumeric(page) Or page=" " Then
page=1
Else
page = (13)
End if
If page<1 Then
page =1
Else If page>maxpage Then
page= (14)
EndIf
rs.AbsolutePage=Page
if page = maxpage Then
x = iCount-(maxpage-1)*iPageSize
else
x= (15)
end If
%>
……
</div>
```

(9)~(15)的备选答案：

A．CInt (page)　B．exec　C．maxpage　D．10

E．EOF　F．iPageSize　G．order

## 5.2.4　同步练习参考答案

【问题 1】

(1) E　(2) B　(3) G　(4) F　(5) C　(6) D　(7) A　(8) H

【问题 2】

(9) B　(10) G　(11) E　(12) A　(13) F　(14) D　(15) C

# 5.3　Web 网站的创建与维护

## 5.3.1　考点辅导

### 5.3.1.1　Web 网站的创建

1. 组织信息

创建 Web 网站时，需要考虑网站的可扩展性、网页技术和网页制作工具的选择，同时还必须考虑网站信息分解、网页链接、主题列表和逻辑顺序等，确保做好网站规划。

2. 构建网站框架

构建网站框架时可以考虑采用布告板、单页线性、多页线性、分层和网状等逻辑组织形式，以提高网站的编码效率。

3. 建立 Web 服务器

1)　Web 服务器简介

Web 服务器是用来存储网页并响应执行用户的访问请求的设备。Web 服务器对通过因特网使用 HTTP 协议的文件、文件夹以及其他资源的访问进行管理，当前最流行的两种 Web 服务器是运行于 Linux 操作系统平台上的 Apache Web 服务器和运行于 Windows 操作系统平台上的 Microsoft 的 IIS Web 服务器。

获得 Web 服务器空间的方式主要包括企业或单位自建和托管 Web 主机两种方式。企业或单位安置服务器需要相应的硬件、软件，还需要相关的人员来架设并维护 Web 服务器。

2)　IIS Web 服务器

利用 IIS 的主要功能可以设置个人 Web 服务器，在工作组中共享信息，访问数据库，开发企业 Intranet 和开发 Web 应用程序。

用户可以通过 Windows 的计算机管理控制台或通过编写脚本来管理 IIS。还可以使用控制台，通过 Web 与他人共享使用 Internet 信息服务管理的站点和服务器的内容。从控制台访问 Internet 信息服务器，可以配置最常用的 IIS 设置和属性。开发站点和应用程序之后，可以在运行功能更加强大的 Windows Server 环境中使用这些设置和属性。

4. 域名注册

域名解析服务器主要负责将 Web 或其他服务器域名解析为相应的 IP 地址。选择适当

的域名后，就可以到中国互联网络信息中心进行注册域名，并签订相应的域名注册协议。

5. Web 网站发布

网站发布之前需要准备 Web 服务器的相关信息，主要包括 Web 服务器协议、URL 地址、服务器文件系统规则和服务器账号等。实施 Web 发布时，可以采用 FTP 工具将网站文件从本地传输到远程服务器上。

#### 5.3.1.2 Web 网站的维护

1. 网站维护

网站维护主要涉及网站系统平台维护和网站内容更新维护两个主要方面。

2. 网站测试

网站测试的主要内容包括浏览器的可变性、不同的分辨率和链接的有效性等。

## 5.3.2 典型例题分析

**例 1** 请根据网页显示的效果图和网页中的元素说明，将 HTML 文本中各空格处的解答填入对应的答案栏内。

**【说明】**

在浏览器的地址栏中输入常春藤大学招生办公室主页的网址并按 Enter 键后，网页显示的效果如图 5-15 所示。

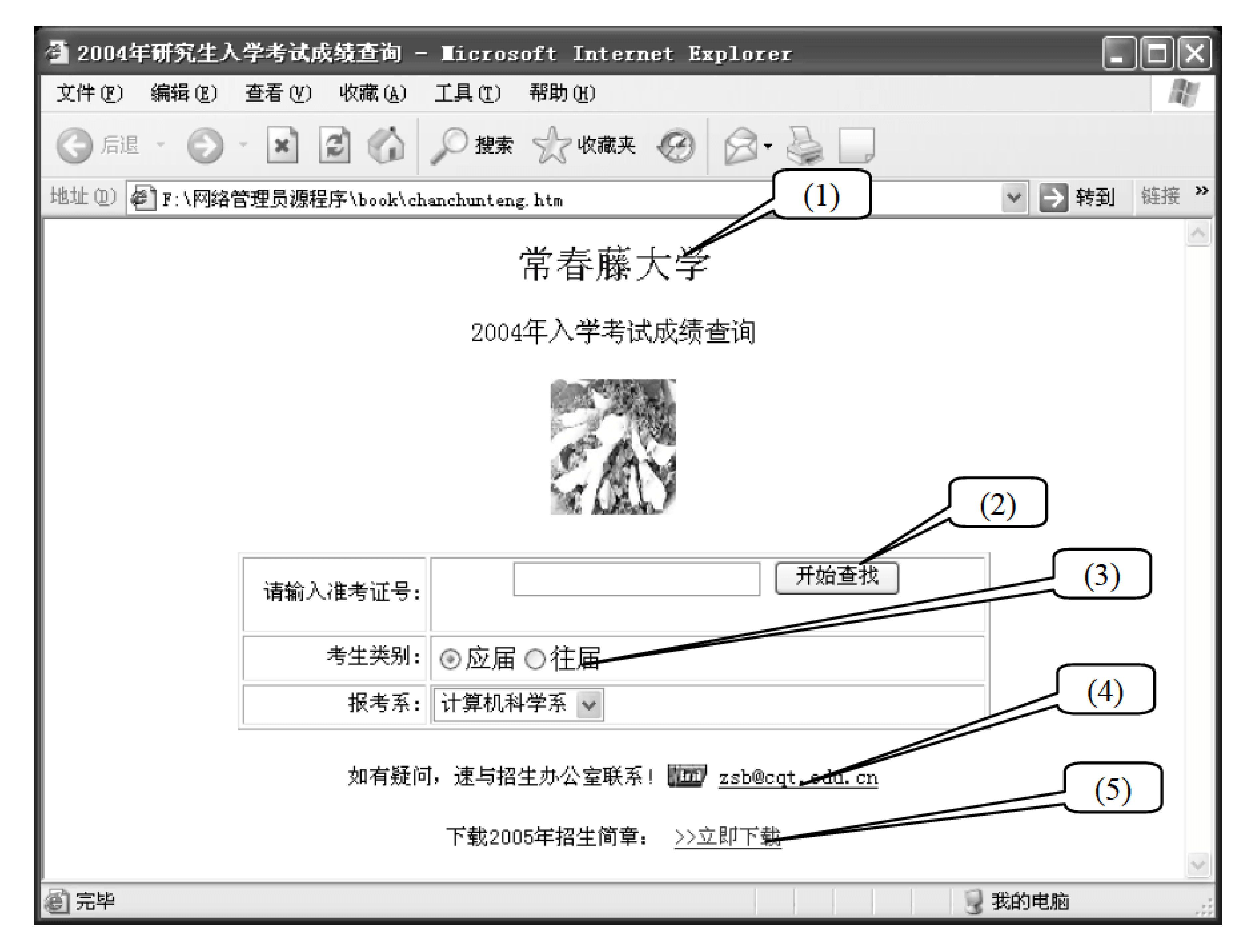



图 5-15 常春藤大学招生办公室主页

网页中的元素说明如表 5-11 所示。

表 5-11　网页中元素说明

| 序　号 | 类　型 | 说　明 |
|---|---|---|
| (1) | 文本 | 内容：常春藤大学；颜色：blue；字体：宋体；字号：5 |
| (2) | 表单 | 方法：post；程序：http://www.server.com/cgibin/program |
| (3) | “考生类别：”选项组 | 名称：“type”；选项：“应届”、“往届” |
| (4) | 动画 | 文件名：animation.gif；高：16；宽：24 |
| (5) | “立即下载”链接 | 文件地址：http://download.cqt.edu.cn/zsjz2005.doc |

HTML 文本如下：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>2004 年研究生入学考试成绩查询</title>
______(1)________

<body  bgcolor="white">
_______(2)_______
</p>
<p align="center">2004 年入学考试成绩查询</p>
<p align="center"><img src="nyc.jpg" width="77" height="83">
</p>
<div  align="center" style="width:679; height:101 ">
<table width="63%" height="17" border="1" >
   <tr>
     <td width="23%" height="1">
      <p align="right"><font face="宋体" size="2">请输入准考证号:</font></p>
      </td>
     <td width="46%" height="1">
    ________(3)_________
      <p align="left">
      <input type="text" name="T1" size="20">
      <input type="submit" value="开始查找" name="B1"></p>
      </form>
      </td>
   </tr>
   <tr>
     <td width="23%" height="17">
      <p align="right"><font size="2">考生类别:</font></p>
      </td>
     <td width="38%" height="19" align="left">
_______(4)________
      </td>
   </tr>
   <tr>
     <td width="23%" height="1">
```

```
          <p align="right"><font size="2">报考系:</font></p>
          </td>
         <td width="46%" height="1">
          <p align="left"><select  size="1" name="D1">
          <option selected>计算机科学系</option>
          <option>机械工程系</option>
          <option>中文系</option>
         </select>
          </p>
          </td>
       </tr>
    </table>
</div>
<p align="center"><font size="2">如有疑问，速与招生办公室联系!
________(5)________
<a href="mailto:vipmail@cqt.edu.cn">zsb@cqt.edu.cn</a></font>
</p>
<p align="center"><font size="2">下载 2005 年招生简章：</font>
________(6)________
<font size="2" color="red"> &gt;&gt;立即下载</font></a></p>
</body>
</html>
```

**分析：**本题主要考查考生对 HTML 网页元素标签的掌握情况。

HTML 元素主要包括基本标签(如字体)、列表、超级链接、图像、图像映射、表格、多媒体、表单和框架等。本题中主要涉及字体、表单、单选按钮、图像和文档下载的超级链接等基本元素。

**答案：**

(1) </head>

(2) <font color="blue" face="宋体" size="5">常春藤大学</font>

(3) <form name="frmSearch"method="post"action="http://www.server.com/cgibin/ program">

(4) <input name="type" type="radio" value="应届" checked>应届
<input name="type" type="radio" value="往届">往届

(5) <img src="animation.gif" width="24" height="16" align="absmiddle">

(6) <a href="http://download.cqt.edu.cn/zsjz2005.doc">

## 5.3.3 同步练习

请根据网页显示的效果图(见图 5-16)和网页中的元素说明，将 HTML 文本中各空格处的解答填入对应的答案栏中。

网页中元素说明如表 5-12 所示。

表 5-12　网页中元素说明

| 序　号 | 类　型 | 说　明 |
|---|---|---|
| (1) | 网页标题 | 文本：Form 表单示例 |
| (2) | 表单对象 | Name：frmLogin；method：post；action：login.aspx |
| (3) | 输入文本框 | Name：txtUser；Id：txtUser |
| (4) | 文本标签 | Label：class：style1；文本：密 码 |
| (5) | 复选框 | Checkbox：checked；name：eem |

这是一个简单的 HTML 文档，显示的是一个网页列表信息，显示界面如图 5-16 所示。

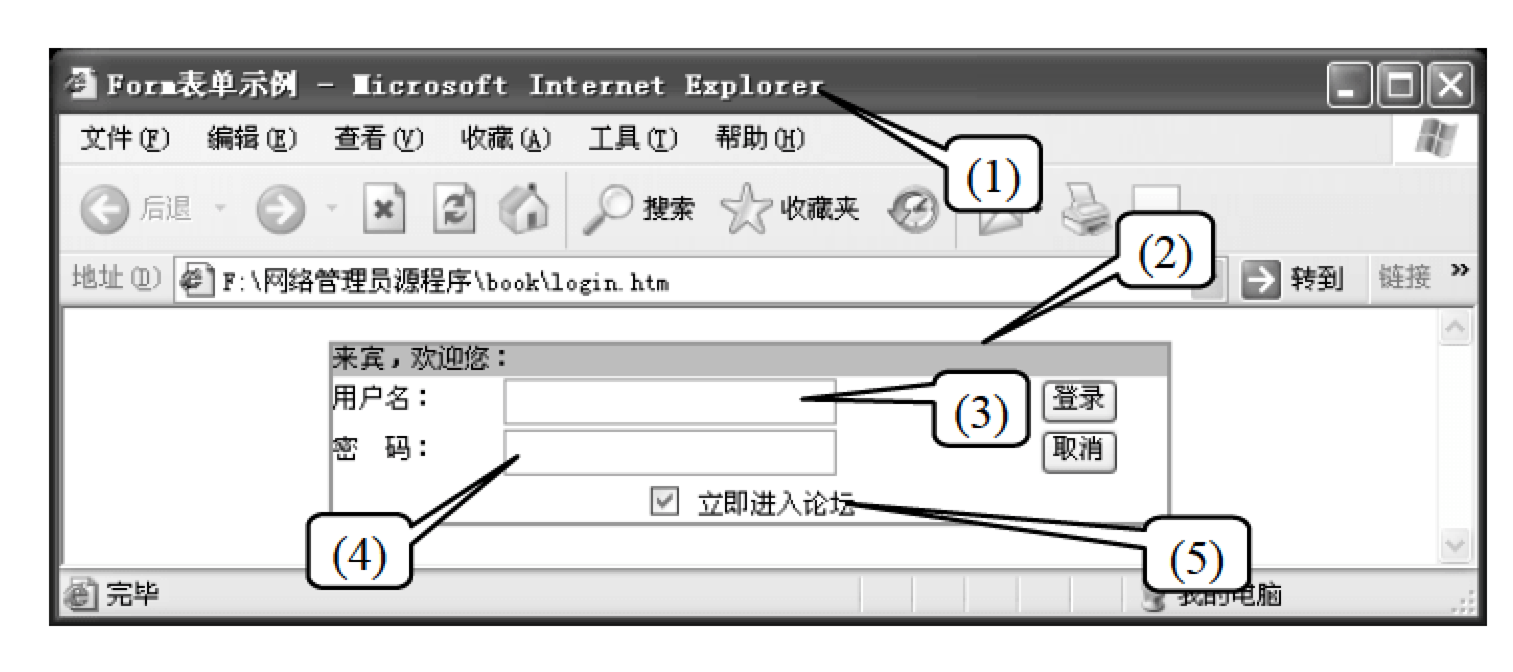



图 5-16　论坛网页

下面是这个论坛页面的 HTML 代码：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
____(1)____
<style type="text/css">
<!--
.style1 {
    font-family: "宋体";
    font-size: 12px;
}
-->
</style>
</head>
<body>
__________(2)__________
  <table width="200" border="1" align="center" cellpadding="0"
cellspacing="0" bordercolor="#CC9900">
    <tr>
    <td>
    <table width="381" border="0" align="center" cellpadding="0"
cellspacing="0" bordercolor="#D4D0C8">
```

```
    <tr>
      <td colspan="3" bgcolor="#CCCC00" scope="col"><span class="style1">
来宾，欢迎您：</span></td>
     </tr>
    <tr>
      <td scope="col"><label class="style1">用户名：</span></label></td>
      <td scope="col">______(3)______</td>
      <td scope="col"><div align="left">
        <input name=btnLogin type=submit id="btnLogin" style="FONT-SIZE:
12px" value=登录>
      </div></td>
    </tr>
    <tr>
      <td>______(4)______</td>
      <td><input name="txtPasswd" type="text" id="txtPasswd"></td>
      <td><input name=btnLogin type=submit id="btnLogin" style="FONT-SIZE:
12px" value=取消></td>
    </tr>
    <tr>
      <td colspan="3"><div align="center" class="style1">
          _______(5)_______
      立即进入论坛</div></td>
    </tr>
  </table>
    </td>
  </tr>
  </table>
</form>
</body>
</html>
```

## 5.3.4 同步练习参考答案

(1) <title>Form 表单示例</title>
(2) <form name="frmLogin" method="post" action="login.aspx">
(3) <input name="txtUser" type="text" id="txtUser">
(4) <label class="style1">密 码：</label>
(5) <input type=checkbox checked name=eem>

# 5.4 本 章 小 结

本章知识点在 2009 年的新大纲中改动不大，主要删除了 XML 动态网页编程技术知识点，新增了 ADO 的概念和实用的知识点。

本部分内容主要要求考生掌握 Web 网站建设的相关内容，包括 HTML 的基础知识，

HTML 应用，网页制作工具使用，动态网页技术以及 Web 网站的建立、管理和维护等 Web 基础知识和应用实现等内容。对 Web 网站建设的学习关键要充分掌握 HTML 的基础知识，以常用的 HTML 元素为主线，抓住重点，熟悉 Web 网站建设中的动态网页技术使用和网站管理与维护等相关内容。

本章内容为下午科目的重点内容，为每年的必考内容。本章的每小节中组织了大量的针对水平考试的典型例题分析和同步训练，这些题目涵盖了大纲规定的知识要点。

# 5.5　达标训练题及参考答案

## 5.5.1　达标训练题

要定义显示一个图 5-17 所示的网页表格，相关信息参考下面的网页说明。将 HTML 文本中各空格处的解答填入对应栏中。

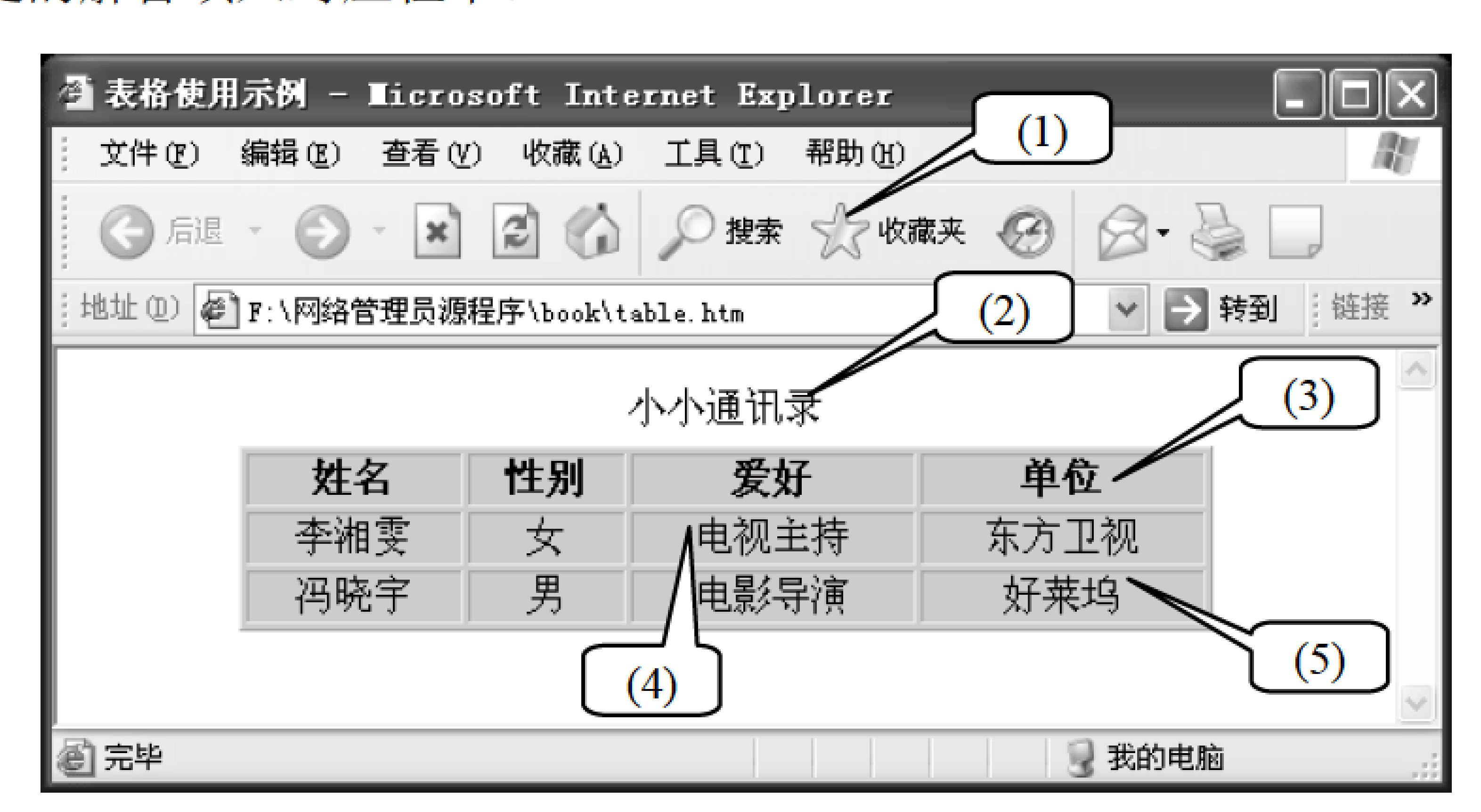



图 5-17　表格在浏览器中打开的效果

网页中各元素的说明如表 5-13 所示。

表 5-13　网页中各元素的说明

| 序　号 | 类　型 | 说　明 |
|---|---|---|
| (1) | 网页标题 | 文本：表格使用示例 |
| (2) | 表格标题 | 文本：小小通讯录 |
| (3) | 单元格标题 | 内容：单位　　　　对齐方式：居中 |
| (4) | 单元格内容 | 内容：电视主持　　对齐方式：居中 |
| (5) | 表格结束 | 表格结束 HTML 标签 |

HTML 文本如下：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
```

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
_____________(1)_____________
</head>
<body>
<table width="200" border="1" bgcolor="#CCCCCC" align="center">
_____________(2)_____________
<thead>
  <tr>
    <th align="center">姓名</th>
    <th align="center">性别</th>
    <th align="center">爱好</th>
    ___________(3)___________
  </tr>
 </thead>
 <tbody>
  <tr>
    <td align="center">李湘雯</td>
    <td align="center">女</td>
    ___________(4)___________
     <td align="center">东方卫视</td>
  </tr>
  <tr>
    <td align="center">冯晓宇</td>
    <td align="center">男</td>
    <td align="center">电影导演</td>
     <td align="center">好莱坞</td>
  </tr>
 </tbody>
___________(5)___________
</body>
</html>
```

## 5.5.2 参考答案

(1) <title>表格使用示例</title>

(2) <caption>小小通讯录</caption>

(3) <th align="center">单位</th>

(4) <td align="center">电视主持</td>

(5) </table>

# 参 考 文 献


[1] 全国计算机技术与软件专业技术资格(水平)考试办公室编．网络管理员教程[M]. 3 版．北京：清华大学出版社，2009.

[2] 全国计算机技术与软件专业技术资格(水平)考试办公室编．网络管理员考试同步辅导[M]．北京：清华大学出版社，2005.

[3] 全国计算机技术与软件专业技术资格(水平)考试办公室编．2009 年网络管理员考试大纲与培训指南(2009 版)[M]．北京：清华大学出版社，2009.

[4] 全国计算机技术与软件专业技术资格(水平)考试办公室编．网络管理员历年试题分析与解答[M]．北京：清华大学出版社，2008.

[5] 全国计算机技术与软件专业技术资格(水平)考试办公室编．网络工程师历年试题分析与解答[M]．北京：清华大学出版社，2008.

[6] 雷震甲．网络工程师教程[M]．3 版．北京：清华大学出版社，2009.

[7] 谢希仁．计算机网络[M]．5 版．北京：电子工业出版社，2009.

[8] 李保华，李敏．局域网组建与维护(2009 版)[M]．北京：清华大学出版社，2009.

[9] 王俊伟，吴俊海．Linux 标准教程[M]．北京：清华大学出版社，2006.

[10] 冉林仓．Red Hat Linux 9 编程开发与网络管理[M]．北京：电子工业出版社，2006.

[11] 王全国，等．网管实战宝典：Windows Server 2003 配置与管理[M]．北京：清华大学出版社，2008.

[12] 斯托林斯，等．网络安全基础：应用与标准[M]．3 版．北京：清华大学出版社，2007.

[13] 唐正军，等．入侵检测技术[M]．北京：清华大学出版社，2008.

[14] 鲍威尔．数据库设计入门经典[M]．北京：清华大学出版社，2007.

[15] 白中英，等．计算机组成原理[M]．北京：科学出版社，2008.

[16] 汤子瀛．计算机操作系统(修订版)[M]．西安：西安电子科技大学出版社，2001.

[17] 康雁，等．计算机专业英语：使用文案(档)写作[M]．北京：清华大学出版社，2009.

[18] 胡静，等．ASP.NET 动态网站开发教程[M]．2 版．北京：清华大学出版社，2009.

[19] 计算机信息网络国际联网安全保护管理办法(1997 年 12 月 30 日中华人民共和国公安部令第 33 号发布).

[20] 计算机信息系统安全专用产品检测和销售许可证管理办法(1997 年 12 月 12 日公安部令第 32 号发布).

[21] 计算机信息系统国际联网保密管理规定(2000 年 1 月 25 日国家保密局国保发[1999]10 号发布).

[22] 中华人民共和国计算机信息系统安全保护条例(1994 年 2 月 18 日中华人民共和国国务院令第 147 号发布).